THALES

Operator Terminal Adapter

OTA

Security Target

Classification	Document Title	Radical – Business Id	Revision	DTC	Language	Entity Cage Code	Thales Cage Code	PAGE
Unclassified	**Security Target for OTA**	**3AQ 24863 AAAA**	**6.2.9**	**377**	**[EN]**	**N4244**	**0026**	**1 of 48**

THALES

DOCUMENT CHANGE HISTORY

Revision	Date	Description
6.2.8	07 Mar 2016	ST referencing Common Criteria V2.3, August 2005
6.2.9	25 Mar 2019	ST updated for Common Criteria V3.1, Release 4, September 2012

	–	6.2.8	6.2.9	003	004	005	006
Written by		**Vidar Karlsen**	**Vidar Karlsen**				
Checked by	QA Manager	**Ole Johnny Pedersen**	**Trine Granby**				
Approved by	PDA	**Pål Taraldsen**	**Pål Taraldsen**				

THALES

Table of Contents

1. SECURITY TARGET INTRODUCTION (ASE_INT)

1.1 Security Target reference

(1) The Security Target is consistent with Common Criteria as specified in ref. [2], [3] and [4].

(2) The following table identifies the Security Target (ST).

Item	**Identification**
ST title	Security Target for OTA
ST reference	3AQ 24863 AAAA 377 EN
ST version	6.2.9
ST author	Thales Norway AS

1.2 Referenced documents

Ref	Id	Title
[1]	AC/35-D/2001-REV2	NATO Security Committee - Directive on Physical Security Note: replaces C-M(55)15(Final), Enclosure C.
[2]	CCMB-2012-09-001	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 revision 4, Part 1 (also known as part 1 of the ISO/IEC 15408 Evaluation Criteria).
[3]	CCMB-2012-09-002	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 revision 4, Part 2 (also known as part 2 of the ISO/IEC 15408 Evaluation Criteria).
[4]	CCMB-2012-09-003	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 revision 4, Part 3 (also known as part 3 of the ISO/IEC 15408 Evaluation Criteria).

1.3 TOE reference

(1) The following table identifies the Target Of Evaluation (TOE)

Target of Evaluation (TOE) Identification	Operator Terminal Adapter (OTA); comprising: • OTA hardware: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B • OTA Trusted Kernel: 3AQ 24860 AAAA version 6.2.5
TOE Assurance Level	EAL5 augmented with ALC_FLR.3
TOE Developer	Thales Norway AS

1.4 TOE overview

(1) The OTA is part of the Voice Communication System (VCS) used in operation sites. The Operator Controller Position (OCP) in the VCS are used by the operators to communicate with aircraft and naval forces afloat via G-A-G or G-M-G radio, other site operators, higher and lower echelons and other authorities and subscribers via G-G communications.

(2) The VCS provides secure and non-secure voice communications to operators in the operation sites, between operators and external military and civilian networks and between operators and radios where that is required. The system is designed to provide a continuous 24 hours operation 7 days a week during times of peace, crisis/tension and war.

(3) The main purpose of the OTA is to provide the capabilities required to handle all voice presented at the OCP and to perform the required red/black separation of voice and data. The OTA connects each OCP to both the secure and non-secure switching networks. The OTA is also used between the management system and the secure / non-secure switching networks so that the management system can manage both the secure and non-secure part of the VCS.

(4) TEMPEST certification is outside the scope of this document.

1.5 TOE description

1.5.1 General

(1) This section presents an overview of the OTA, and the perimeter of the TOE within the OTA, to assist potential users in determining whether it meets their needs.

1.5.2 OTA in VCS

(1) Figure 1-1shows the OTA in the VCS. OTA is used in two configurations in the VCS, namely:

(a) OTA in OCP (in the Operator Position Subsystem in the figure)

(b) OTA for SMA (in the Access Network Subsystem in the figure)

(2) The two configurations have identical hardware and software. The mode of operation is determined by an installation parameter. OTA in OCP mode has audio handling and must have a lamp panel connected in order to handle audio. OTA for SMA does not have audio handling and has no lamp panel connected.

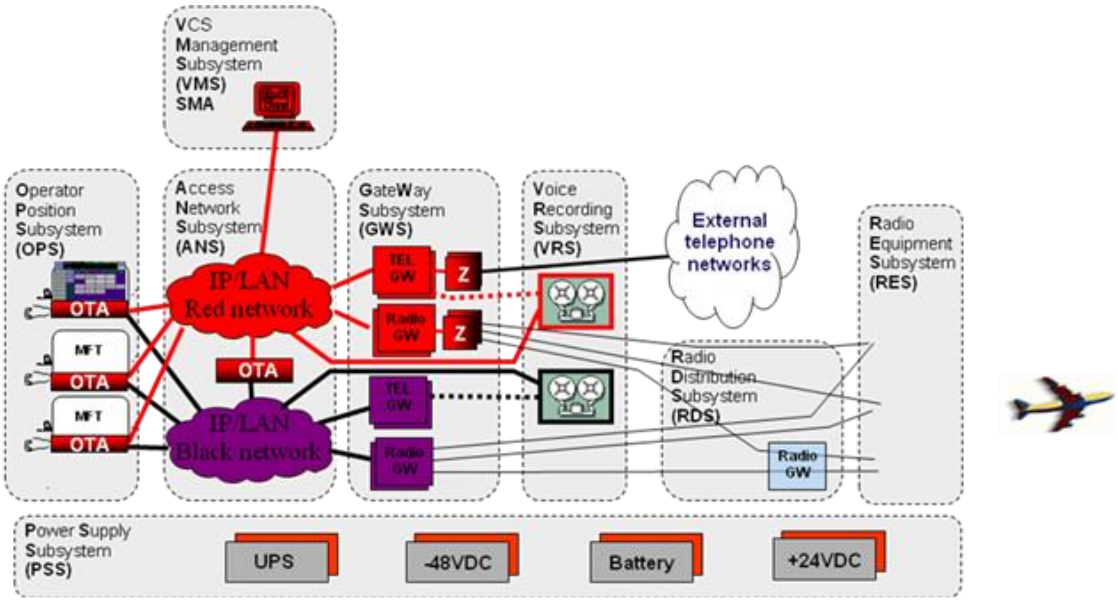

Figure 1-1 VCS architecture

1.5.3 Definition of TOE perimeter

(1) The TOE is the parts of the OTA implementing the core security functions, which must be highly trusted. The TOE is defined in section 1.3 “TOE reference” and comprises:

(a) The complete OTA HW; and

(b) One software configuration item comprising a defined set of OTA software modules.

(2) The TOE software consists of:

(a) The firewall including drivers (the firewall configuration file is outside the TOE, ref. (3) below);

(b) Boot software and software loader; and

(c) The red/black separation software including task switching; and

(d) Digital Signal Processor (DSP) SW

(3) The configuration of the firewall is set when the TOE SW is compiled and linked, thus making the configuration fixed and not possible to change during runtime. To change configuration a new TOE SW must be loaded. The customized configuration parameters are read from a firewall configuration file which is part of the OTA application software, i.e. outside the TOE.

(4) The OTA application software is running in the secure and non-secure software tasks as illustrated in Figure 1-2 showing the OTA architecture. The OTA application software is considered less security critical and is outside the TOE, ref. ch. 1.6.1.

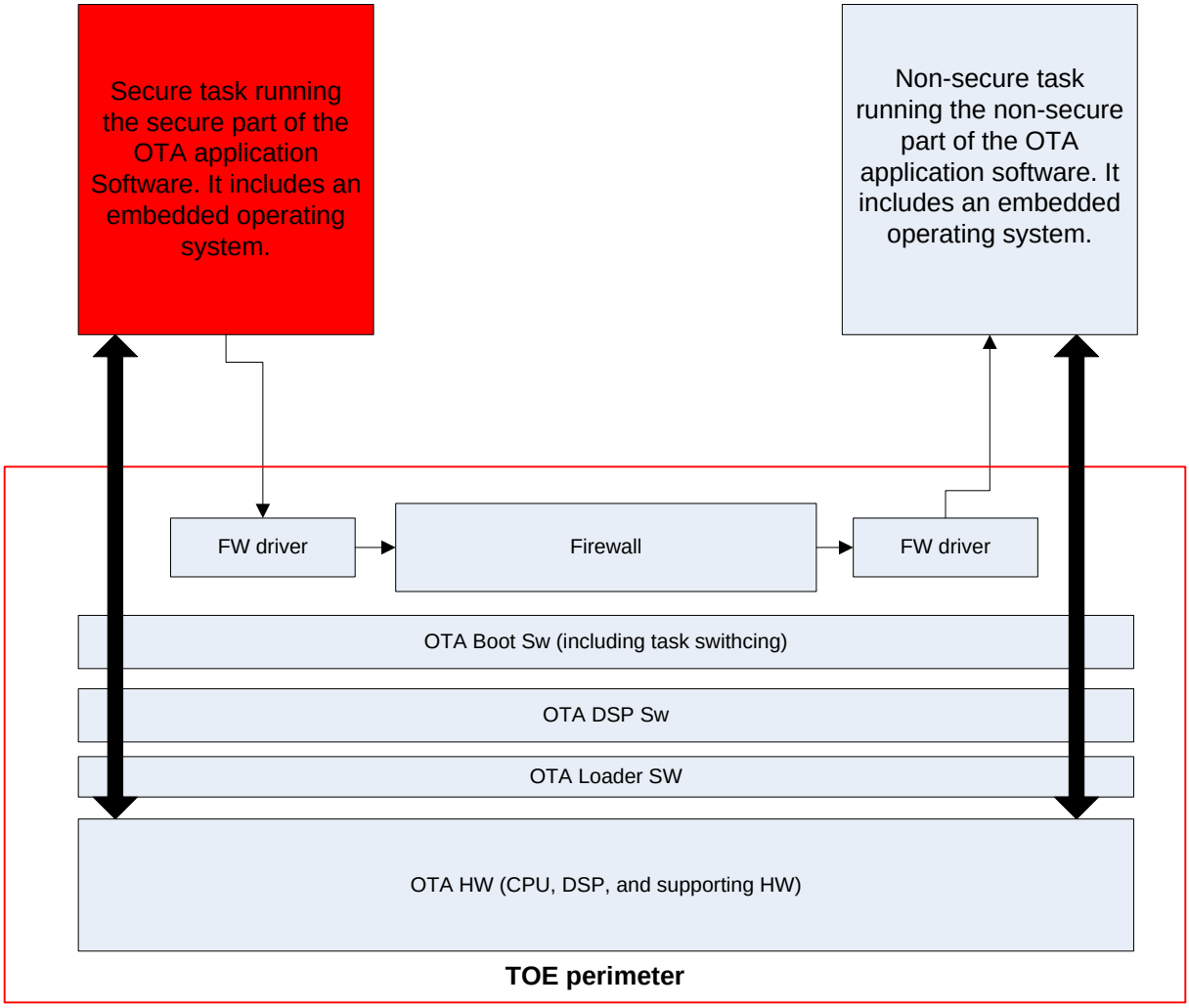

Figure 1-2 OTA architecture

(5) For the rest of this document the term OTA is used when referring to the OTA as a whole, the term TOE is used when referring to the TOE as defined in this section. The term OTA application is used when referring to the OTA software that is outside the TOE.

1.5.4 The TOE HW

(1) The TOE HW provides connection for the audio devices, the loudspeaker and lamps and the Ethernet interfaces, as shown in Figure 1-3 below.

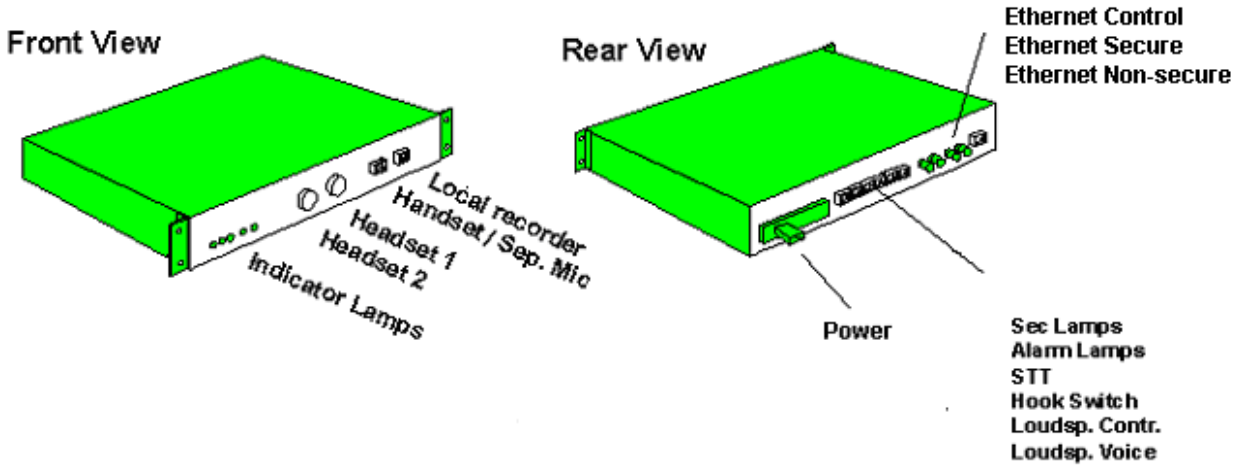

Figure 1-3 TOE physical interfaces

(2) The main functions of the TOE HW are to process voice, and to perform red/black separation. The TOE uses an external AC/DC converter. All connectors that may be used by OCP users are located at the front of the TOE; while all connectors intended to be handled by installation and maintenance are located at the rear end. The front end has also some indicator lamps providing information of the status of the TOE, the power and each of the Ethernet interfaces.

(3) The OCP has both handset and headset, but only one at a time can be active.

(4) The OCP supervisor feature is provided by use of a second headset. The voice from the microphone in one headset is sent back into the ear of the other headset. The microphone voice to be sent by the TOE towards the communication resources is a sum of the microphone voice from the two headset microphones.

(5) The handset connector can also be used for a separate microphone. The intended use is for personnel wearing NBC gear. The headset connector #1 is then used to connect the headset.

(6) The TOE is connected to secure and non-secure LAN by use of 100 Mb/s Ethernet interface on fibre and can be connected to the MFT via a 10/100 Mb/s electrical Ethernet interface (called Ethernet Control in Figure 1-3).

(7) The TOE HW is equipped with a physical sealing that functions as a passive protection mechanism.

1.5.5 The TOE SW

(1) The TOE SW as defined in section 1.3 performs the following main functions:

(a) Firewall

The firewall, which is configured at SW compile time by a customer specific firewall definition file (see ch. 1.5.3 pts. 2 & 3), checks all messages from secure to non-secure domain (see fig. 1-2) and accepts messages compliant with the preset configuration.

(b) Red/black separation

Red/black separation is mainly achieved by separation of the secure (red) and non-secure (black) data and application SW in the OTA.

(c) SW loader, HW initialisation, self-tests, start-up and task switching functions.

(d) DSP with echo cancelling and VoX functions.

1.5.6 Voice reception

(1) The OTA receives voice from different connections for the different voice communication services, as shown in Figure 1-4 below:

(a) The radio communication service provides connections from the Radio Gateway

(b) The telephone communication service provides connection from the TGW

(c) The intercom communication service provides connections from other OCPs

(d) The loop monitoring communication service provides connections from the TGW

(2) The allocation of these voice connections to the different voice output devices are controlled from MFT.

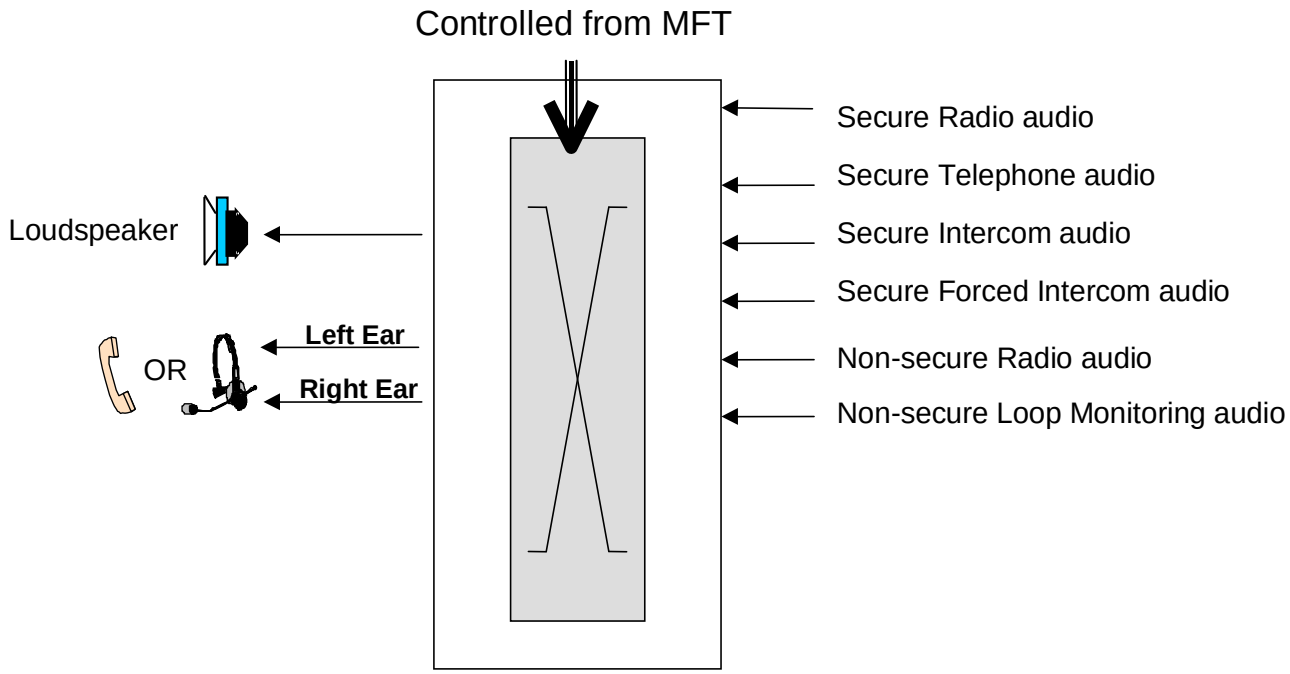

Figure 1-4 Audio presentation capabilities

(3) The voice handling capacity for voice reception in the OTA is the combination of secure and non-secure voice connections. To avoid unwanted acoustic cross-talk, secure voice reception will in some cases be muted. When the handset is used, secure voice reception will be muted when the microphone is connected to a non-secure connection. Similarly if the separate microphone is used, the secure voice reception will be muted when the microphone is connected to a non-secure connection.

(4) The voice sent to the loudspeaker shall be non-secure only.

(5) When the handset is used (i.e. off-hook), the voice for the left and right ear is summed before sent to the handset. The voice to the headset can be configured from the MFT to be sent in mono; i.e. the same voice is sent to both ears.

1.5.7 Voice transmission

(1) The OTA sends voice to different connections for the different voice communication services, as shown in Figure 1-5 below:

(a) The radio communication service provides connection to the Radio Gateway

(b) The telephone communication service provides connection to the TGW

(c) The intercom communication service provides connection to other OCPs; this VoIP connection is used either for the normal intercom or for the forced intercom service

(2) The TOE selects voice from one of the microphone inputs. The voice from the separate microphone is selected if a separate microphone is connected. The voice from the handset microphone is selected when the handset is off-hook. If the handset is on-hook and separate microphone not connected, the voice from the headset microphones is used.

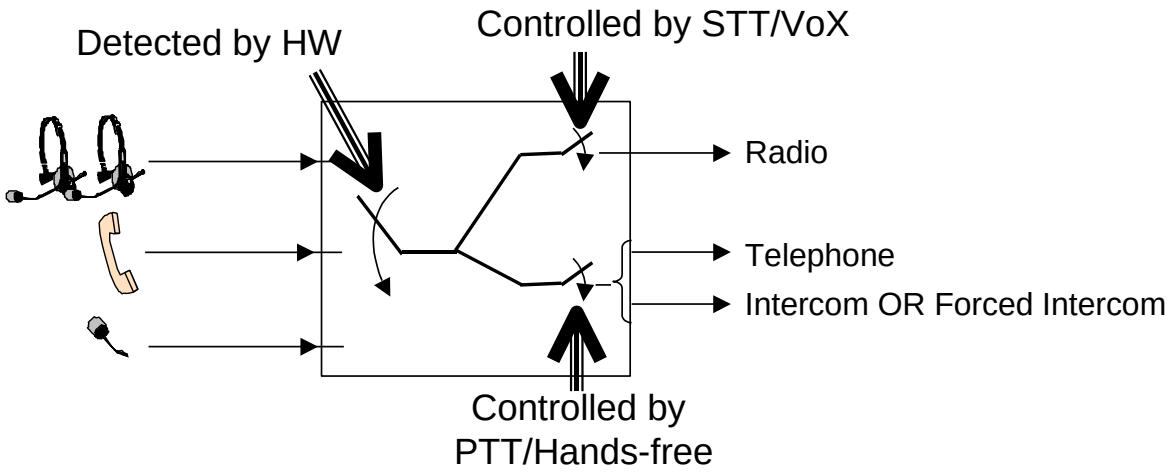

Figure 1-5 Audio transmission capabilities

(3) Transmission of voice on the different channels is controlled by STT, PTT, VoX or can be permanent for a period of time (e.g. handsfree mode for telephone/intercom). An example on how it can be used is described in the following and depicted in Figure 1-5:

(4) The voice from the selected microphone source is then sent to the connections for the different voice communication services depending on the STT/PTT status. STT (i.e. foot-operated PTT) is used to send the voice to the Radio Gateway, while PTT (i.e. hand-operated PTT) is used to send the voice to the telephone gateway for the telephone communication service and another OCP position for the intercom communication service.

(5) If the hands-free capability is selected (from the MFT), the OTA emulates an always-active PTT. The hands-free mode applies to secure telephone and secure intercom connections only. If the OCP user answers or establishes a non-secure telephone call while in hands-free mode, the hands-free mode is automatically disabled.

(6) If the VoX capability is selected (from the MFT), the VoX emulates the STT. This implies that VoX applies to radio communication only.

1.5.8 Audio devices

(1) The audio devices of the OCP position are identified in Figure 1-6 below.

(2) The headset has a PTT button on the cord. The headset and handset microphone provides noise cancelling in order to minimise the pick-up of noise from the neighbouring positions. The handset has a built in PTT button.

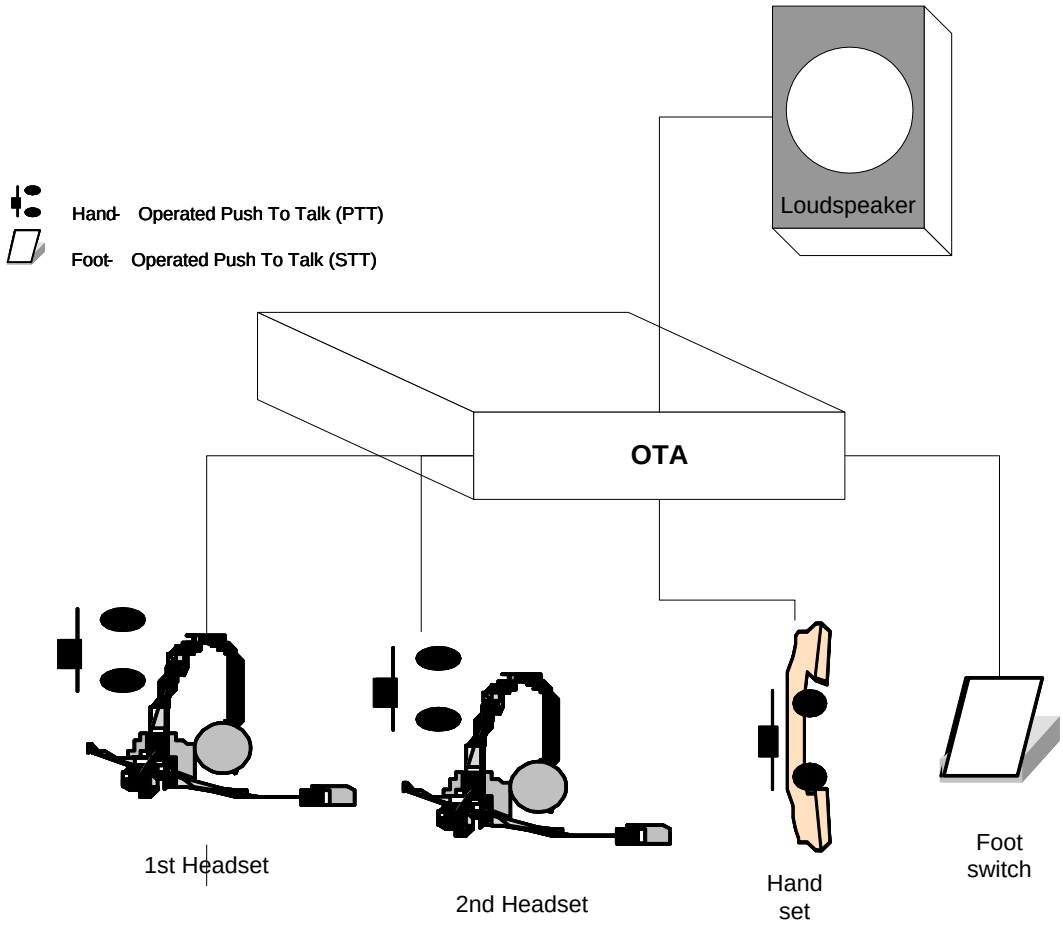

Figure 1-6 Audio devices

1.5.9 Operator Controller Position (OCP)

(1) The OCP consists of the OTA, the MFT, and the LOL with the loudspeaker with on/off switch and volume control and a lamp panel. The MFT consist of a touch display with an integrated PC. The loudspeaker and lamp panel are connected to the OTA. The lamp panel includes 6 lamps showing the security status of the OCP and the security status of neighbour positions, PTT/STT status, power and OTA error status.

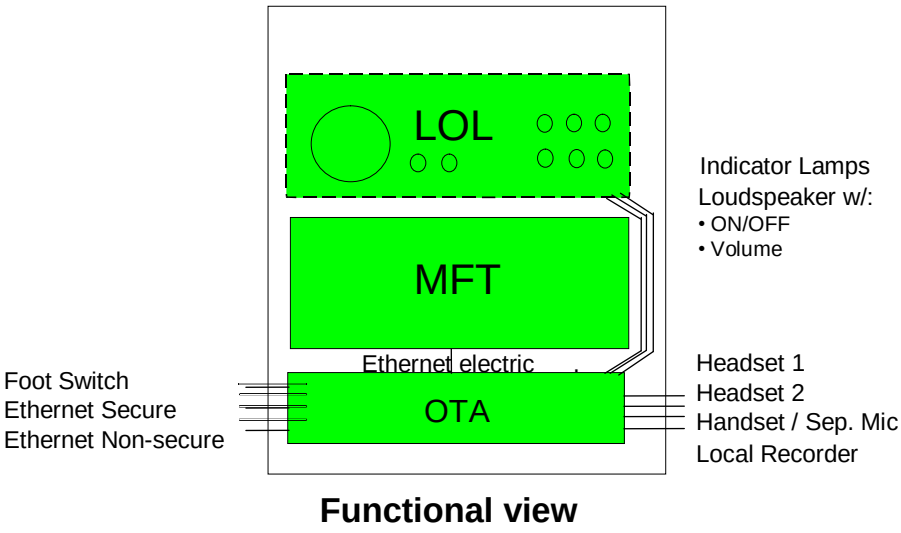

Figure 1-7 Operator Controller Position

1.5.10 Scope of evaluation

(1) The TOE is the parts of the OTA as identified in section 1.3 “TOE reference”

(2) The scope of evaluation is evaluation of security functions in the TOE. These security functions are identified in TOE summary specification.

(3) TEMPEST is not within this scope of evaluation.

1.6 Required non-TOE SW

1.6.1 The OTA application SW

(1) The OTA application SW performs the following main functions:

(a) Voice handling
The OTA application sums the voice that shall be sent to different outputs: left ear, right ear and loudspeaker. The different communication services are configured from the MFT to send the voice to one of the voice outputs. The voice from the microphone is also sent towards the access network. These features are further described in c) below.

(b) Routing
The OTA can have 3 different LAN connected; one MFT LAN, one secure LAN, and one non-secure LAN respectively. This implies that the OTA application must be able to route IP packets.

(c) Recording
TOE supports centralised and local recording of the voice output (i.e. voice to loudspeaker and left and right ear) and the voice input (i.e. microphone voice).

(d) Firewall configuration file
The firewall configuration file is customized at compile time according to operational needs. The customized content defines the behaviour of the firewall with respect to what is allowed to pass from secure to non-secure side. The file resides in the secure part (red) part of the application SW.

(e) Alarm and audit handling
The OTA application will send alarms raised by the TOE to the management system which will provide facilities to securely store the audit data. The audit data are timestamped and logs are generated in an easy readable format available to authorised management operators. The operators shall have special autorisation to gain access to handle audit logs, management, and configuration of the VCS.

(2) When the OTA is configured as OTA in OCP, all functions are used. When the OTA is configured as OTA for SMA, voice handling and recording functions are not used.

1.7 Conventions

(1) The notation, formatting and conventions used in this Security Target are consistent with those used in version 3.1 of the Common Criteria (CC).

(2) The CC functional and assurance components may be used exactly as defined in CC Part 2 and CC Part 3, or they may be tailored through the use of permitted operations as described in CC Part 1, §8.1:

(3) The *assignment* operation occurs when a given component contains an element with a parameter that may be set by the Security Target author. The assignment is indicated by showing the value in square brackets with *italicized and underlined* text. Example:

(a) In CC Part 2 the component FAU_ARP.1.1 calls for an assignment:

(i) The TSF shall take [assignment: list of actions] upon detection of a potential security violation.

(b) The requirement is tailored by the assignment as follows:

(i) The TSF shall take [*an action to raise a local alarm*] upon detection of a potential security violation.

(4) The *selection* operation occurs where a given component contains an element where a choice from several items has to be made by the Security Target author. The selection is indicated by showing the value in square brackets with *italicized* text. Example:

(a) In CC Part 2, requirement FAU_STG.2.2 calls for a selection:

(i) The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

(b) The requirement is tailored by the selection as follows:

(i) The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

(5) The *iteration* operation is used when there is more than one requirement based on the same component. Iteration is denoted by showing the iteration number in parenthesis following the component identifier. Example of how iterations can be used:

(a) If the Security Target should specify two requirements based on FAU_ARP.1 they would be denoted FAU_ARP.1(1) and FAU_ARP.1(2).

(6) The *refinement* operation is performed by altering the requirement. Refinements are indicated by **bold text** and ~~strikethrough~~.

(7) **Assumptions** are given names beginning with “A.”.

(a) Example: A.PHYSICAL

(8) **Threat agents** are given names beginning with “TA.”.

(a) Example: TA.INTERNAL

(9) **Threats** are given names beginning with “T.”.

(a) Example: T.TAMPERING

(10) **Policies** statements are given names beginning with “P.”.

(a) Example: P.COUPLING

(11) **Security objectives** are given names as follows:

(a) IT Security Objectives applicable for the TOE are given names beginning with “O.”.

(i) Example: O.AUDIT

(b) Non-IT Security Objectives applicable for the TOE are given names beginning with “NO.”.

(i) Example: NO.SEALING

(c) IT Security Objectives applicable for the environment are given names beginning with “OE.”.

(i) Example: OE.AUDIT

(d) Non-IT Security Objectives applicable for the environment are given names beginning with “NOE.”.

(i) Example: NOE.INSTALL

2. CONFORMANCE CLAIMS (ASE_CCL)

2.1 CC conformance claim

Conformance	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002 Part 3: Security Assurance Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003
Assurance level	EAL5 augmented with ALC_FLR.3 (Systematic flaw remediation)

2.2 PP and Package conformance claims

(1) The Security Target has no Protection Profile claims.

(2) The Security Target has no Package conformance claims.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1 General

(1) This section provides the statement of the Security Problem Definitions, which identifies and explains all:

(a) Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

(b) Known and presumed threats countered by either the TOE or by the security environment.

(c) Organisational security policies the TOE must comply with.

3.2 Assumptions

(1) The following conditions are assumed to exist in the operational environment.

A.PHYSICAL	The VCS is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
A.TRAINING	All OCP users are trained in the correct use of the VCS facilities.
A.CLEARANCE	All OCP users have a minimum clearance for the highest security level of information handled in the system, and is authorised for all information handled by the system.
A.MAN.AUTHORISED	Only users with special authorisation are allowed to do configuration and management of the system including TOE.
A.VCS.COM	The LANs in the VCS shall not be used for other communication than voice and signalling for call handling and system internal management communication.
A.USAGE	The OTA is used in the VCS and is installed according to the installation guidelines for the VCS.
A.AUDIT	The audit functionality is handled outside the TOE.
A.SELF.TEST	The periodic test of the firewall in the TOE will be initiated from the OTA application.
A.OTA.ALARM	The OTA application will transmit alarms from the TOE to the management system (i.e. SMA) and be presented to the operator at the management system.

3.3 Threats

3.3.1 General

(1) This section identifies the assets, threat agents and threats.

3.3.2 Identification of assets

(1) The assets that TOE shall protect as specified in this Security Target are the following:

(a) Classified information (voice and data) transmitted through the TOE.

3.3.3 Identification of threat agents

TA.INTERNAL	Personnel which have authorised access to the operations site and which has intent to perform unauthorised actions. These persons may be trained specially to perform their unauthorised actions. They may bring unauthorised software into the site and may be able to load it. They may be supported by entities with unlimited resources.
TA.EXTERNAL	Personnel which do not have access to the operations site and which has the intent to divulge classified information. These persons may have unlimited resources.
TA.USER	OCP users with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.TECHNICIAN	Technicians with no intent to perform unauthorised actions. They may unintentionally perform unauthorised actions.
TA.MALFUNCTIONS	System malfunctions. System malfunctions to be considered are limited to single point of failure.

3.3.4 Threats

T.CONN.SEC.NON-SEC	Classified information on a secure channel may be transferred to non-secure channels.
Threat agents	TA.TECHNICIAN, and/or TA.MALFUNCTIONS. In addition the following must be present: TA.EXTERNAL
Asset	Classified information

Unwanted outcome	Unauthorised personnel get access to classified information.
Attack methods	1. A technician (TA.TECHNICIAN) unintentionally configure or install the TOE in a way which transfer information on secure channels (i.e. classified information) to non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area. 2. A malfunction in the TOE implies that information on secure channels (i.e. classified information) is transferred to non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.
T.TAMPERING	Security-critical part of the TOE may be subject to physical attack that may compromise security.
Threat agent	TA.INTERNAL combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	A person (TA.INTERNAL or TA.EXTERNAL) modifies the TOE to transfer information on secure channels (i.e. classified information) to non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.
T.MISUSE	An attacker may send classified information from the secure to the non-secure network, by the use of call handling or management messages.
Threat agent	TA.INTERNAL combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	A person (TA.INTERNAL) introduce/modify software and/or hardware in the secure network to pick up classified information and transfer this information to non-secure channels via the firewall. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area. This threat increases if this can continue undetected.
T.WRONG.SEC.IND	System malfunctions may give the OCP user a wrong indication of whether the microphone is connected to a secure channel or a non-secure channel. The OCP user may then speak classified information on the non-secure network.

Threat agent	TA.USER, TA.MALFUNCTIONS combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	System malfunctions gives the OCP user (TA.USER) an indication that the microphone is not connected to a non-secure channel, while in reality the microphone is connected to a non-secure channel. The OCP user then speaks classified. The classified information is picked up by the microphone and transmitted on a non-secure channel. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.
T.SEC.IND.MISSING	The OCP user speaks classified information when the microphone is connected to the non-secure network
Threat agent	TA.USER combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	This threat will occur if the TOE does not provide the OCP user (TA.USER) an indication of when the microphone is connected to a non-secure channel. When the microphone is connected to a non-secure channel, and the OCP user then speaks classified, then the classified information is picked up by the microphone and transmitted on a non-secure channel. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.
T.ACOUSTIC.PICK-UP	Microphones connected to non-secure channels may pick up classified speech.
Threat agent	TA.USER combined with TA.EXTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	When the microphone is connected to a non-secure channel, and the a person in the room (TA.USER) speaks classified or classified information is presented on audio output devices, then the classified information can be picked up by the microphone and transmitted on a non-secure channel. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.
T.TEMPEST	Electromagnetic emanations may divulge classified information.

Threat agent	TA.EXTERNAL possibly in combination with TA.INTERNAL
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Information on secure channels (i.e. classified information) is electromagnetically emanated onto non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.
T.UNAUTHORISED.USE	Authorised persons may perform unauthorised use of the operator position applications and management system inside the operation site.
Threat agent	TA.INTERNAL or TA.USER. In addition the following must be present TA.EXTERNAL.
Asset	Classified information
Unwanted outcome	Unauthorised personnel get access to classified information.
Attack method	Authorised persons may perform intentionally (TA.INTERNAL) or unintentionally (TA.USER) unauthorised use of the operator position applications and management system inside the operation site. The threat is that this may lead to transfer of classified information onto non-secure channels. The classified information is picked up from the non-secure channels by persons (TA.EXTERNAL) outside the physically protected area.

3.4 Organisational security policies

P.COUPLING	Audio coupling of secure communications onto active non-secure lines at operator consoles shall be avoided in accordance with ref. [1], paragraphs 35 and 37.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1 TOE IT security objectives

O.ALARM.FAILURE	If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm indication and raise an alarm to the OTA application (required non-TOE SW) in order to send an alarm message to the management system. When the TOE operates in the mode “OTA in OCP”, the TOE shall also upon detection of failures on the security indicators (lamp panel), raise a local alarm indication and raise an alarm to the OTA application (required non-TOE SW) in order to send an alarm message to the management system.
O.ALARM.FW	The TOE shall raise an alarm to the OTA application (required non-TOE SW) in order to send an alarm message to the management system when the threshold for traffic through the firewall is exceeded or when messages are rejected by the firewall.
O.CROSS-TALK	To prevent unacceptable acoustic cross-talk, the TOE shall ensure the following: • Secure channels shall be disconnected from the audio outputs when the voice transmission is activated and the microphone is connected to a non-secure channel to prevent unacceptable acoustic cross-talk of voice from secure channels to non-secure voice channels via audio devices connected to the TOE. • The microphone(s) shall be disconnected from non-secure channels when voice transmission is not activated. • The loudspeaker shall not be connected to secure channels. Remark to the term “unacceptable acoustic cross-talk” : The headsets and the use of the headsets shall prevent unacceptable acoustic cross-talk between earpiece and microphone of the headsets. The TOE shall cover all other potential cases of acoustic cross-talk of voice from secure channels to non-secure voice channels via audio devices connected to the TOE.
O.FILTER	Classified information shall be prevented from being transmitted on non-secure channels.

O.SEC.ATTRIBUTES	The TOE shall ensure that only secure (valid) values are accepted for security attributes that are received from the environment.
O.SEC.NON-SEC	Information transmitted on secure voice channels shall not be transferred to non-secure voice channels.
O.SELF.TEST	Security critical functions shall be tested by a combination of power-up tests, periodic tests and/or continuous tests.
O.TX.STATUS	The OCP user shall unambiguously be made aware whether the microphone is connected to a non-secure channel.

4.2 TOE Non-IT security objectives

NO.SEALING	The TOE shall be sealed in such a way that it is easy to see that it has been opened/tampered with.
NO.TEMPEST	TEMPEST evaluation and certification of the TOE is performed by NSM. This certification ensures that NO.TEMPEST is achieved. This aspect is not treated further in this document.

4.3 Environment IT security objectives

OE.AUDIT	The management system shall receive auditable events from the TOE and provide facilities to securely store the audit data and present them for authorised management operators.
OE.MAN.ACCESS	Special authorisation is required to grant access to handle configuration and management of the VCS.
OE.MAN.ALARM	The management system shall receive alarms from the TOE and present them for the management operator.
OE.RECORDING	The voice from the OCP shall be recorded.
OE.SELF.TEST	The periodic test of the firewall in the TOE shall be initiated from the OTA application.

4.4 Environment non-IT security objectives

NOE.ACCESS.CTRL	Only authorised persons shall be given physical access to the VCS.
NOE.AUDIT	Authorised users of the audit facilities must ensure that the audit facilities are used and managed effectively. On particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.
NOE.CCI	The TOE shall be treated as a CCI material.
NOE.CLEARANCE	All OCP users shall have a minimum clearance for the maximum-security level of information handled in the system.
NOE.INSTALL	The responsible for the TOE must ensure that the VCS including the TOE are installed accordingly to the installation guidelines for the VCS.
NOE.MAN.TRAIN	The VCS managers are fully trained to use and interpret the management application for the TOE.
NOE.NEIGHBOURS	Each OCP user shall be made aware of ongoing non-secure transmission on the neighbouring OCPs. Operational procedures, not technical solutions, shall regulate concurrent use of classified and unclassified conversations to prevent acoustic cross-talk of classified conversations to be transmitted on unclassified communication channels.
NOE.PHYS. PROT	The VCS site shall have physical protection, which is minimum approved for the highest level of information handled in the system.
NOE.USER.TRAIN	The OCP users are fully trained to use the OTA and interpret the lamps on the LOL.

4.5 Security objectives for the TOE rationale

Threats/ Assumptions / Objectives	P.COUPLING	T.CONN.SEC.NON-SEC	T.TAMPERING	T.MISUSE	T.WRONG.SEC.IND	T.SEC.IND.MISSING	T.ACOUSTIC.PICK-UP	T.TEMPEST	T.UNAUTHORISED.USE	A.OTA.ALARM	A.SELF.TEST	A.PHYSICAL	A.TRAINING	A.CLEARANCE	A.MAN.AUTHORISED	A.VCS.COM	A.USAGE	A.AUDIT
O.ALARM.FAILURE		x			x													
O.ALARM.FW				x														
O.CROSS-TALK	x	x					x											
O.FILTER				x														
O.SEC.ATTRIBUTES				x					x									
O.SEC.NON-SEC	x	x																
O.SELF.TEST		x			x													
O.TX.STATUS						x												
NO.SEALING			x															
NO.TEMPEST		x						x										
OE.AUDIT																		x
OE.MAN.ACCES									x						x			
OE.MAN.ALARM		x		x						x								
OE.RECORDING									x									
OE.SELF.TEST		x									x							
NOE.ACCESS.CTRL												x		x				
NOE.AUDIT																		x
NOE.CCI			x										x					
NOE.CLEARANCE														x				
NOE.INSTALL		x						x				x	x			x	x	x
NOE.MAN.TRAIN		x		x									x					
NOE.NEIGHBOURS							x											
NOE.PHYS.PROT			x									x						
NOE.USER.TRAIN		x			x	x			x				x					

Table 4-1 Mapping of Objectives to Threats and Assumptions

4.5.1 General

(1) As can be seen from Table 4-1, at least one objective, either TOE or environment, as applicable meets all threats and assumptions. The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

4.5.2 P.COUPLING

(1) The TOE controls the separation of non-secure and secure information and the information flowing from the audio interfaces to/from the non-secure/secure networks (O.SEC.NON-SEC). The audio handling on the TOE will block secure information to the audio outputs, when there is a possibility that non-secure microphones may pick up classified information (O.CROSS-TALK).

4.5.3 T.CONN.SEC.NON-SEC

(1) The TOE controls the separation of non-secure and secure information and the information flowing from the audio interfaces to/from the non-secure/secure networks (O.SEC.NON-SEC). The audio handling on the TOE will block secure information to the audio outputs, when there is a possibility that non-secure microphones may pick up classified information (O.CROSS-TALK). The TOE will eliminate the threat that classified information can exist on the loudspeaker that could be picked up by non-secure microphones (O.CROSS-TALK). A failing in domain separation will be detected during power-up and/or normal operation (O.SELF.TEST, OE.SELF.TEST)). A local alarm indication is given by detection of hardware or software failure (O.ALARM.FAILURE). The alarm is reported to the management system (if possible) which will raise an alarm to the management operator (OE.MAN.ALARM). All users of VCS are fully trained to use, handle and interpret the VCS equipment (NOE.USER.TRAIN), (NOE.MAN.TRAIN). The TOE is installed (NOE.INSTALL) and given TEMPEST protection (NO.TEMPEST) according to established guidelines.

4.5.4 T.TAMPERING

(1) To prevent tampering the TOE is installed in physical protected area that is provided with access control system (NOE.PHYS.PROT). The TOE is also sealed, so it is easy to see that the seal has been broken (NO.SEALING). Periodical manual inspection will detect possible tampering (NOE.CCI).

4.5.5 T.MISUSE

(1) The TOE will receive firewall traffic threshold from the management system and ensure that only valid values are accepted (O.SEC.ATTRIBUTES). All messages from the secure network to the non-secure network are checked in the TOE firewall (O.FILTER). The firewall will report an alarm to the management system if it discovers possible unauthorised use of channels or if a message is rejected (O.ALARM.FW). The management system will then raise alarm to the management

operator (OE.MAN.ALARM). The manager is trained to respond correctly to the firewall alarm (NOE.MAN.TRAIN) to stop any attempt to misuse the channels through the firewall.

4.5.6 T.WRONG.SEC.IND

(1) If a security indicator to the OCP user fails, the TOE will block the signals from the microphone to the non-secure network (O.SELF.TEST). A local alarm is always given by detection of hardware or software failure (O.ALARM.FAILURE). All OCP users are fully trained in the correct use and interpretation of the TOE (NOE.USER.TRAIN).

4.5.7 T.SEC.IND.MISSING

(1) The OCP user shall always have a clear indication whether the microphone is connected to the secure or non-secure network (O.TX.STATUS). All OCP users are fully trained in the correct use and interpretation of the TOE (NOE.USER.TRAIN).

4.5.8 T.ACOUSTIC.PICK-UP

(1) The audio handling on the TOE will block secure information to the audio outputs, when there is a possibility that non-secure microphones on the TOE may pick up classified information (O.CROSS-TALK). The TOE will eliminate the threat that classified information can exist on the loudspeaker that could be picked up by non-secure microphones (O.CROSS-TALK). To prevent acoustic pick up from neighbouring OCP users, each OCP user is made aware of ongoing non-secure transmission on the neighbouring OCPs (NOE.NEIGHBOURS). The TOE will minimise the risk that non-secure microphones can pick up classified information by blocking the microphone when not used (O.CROSS-TALK).

4.5.9 T.TEMPEST

(1) The TOE shall be installed according to VCS installation guidelines (NOE.INSTALL), which complies with the TEMPEST installation guidelines. NSM performs TEMPEST evaluation and certification of the TOE (NO.TEMPEST).

4.5.10 T.UNAUTHORISED.USE

(1) Users need special authorisation to handle the configuration and management part of the VCS (OE.MAN.ACCES), and all received security attributes are checked by the TOE (O.SEC.ATTRIBUTES). The voice from the OCP will be recorded and unauthorised use can be exposed (OE.RECORDING). All OCP users are fully trained in the correct use and interpretation of the TOE (NOE.USER.TRAIN).

4.5.11 A.OTA.ALARM

(1) The OTA application will transmit alarms (if possible) to the management system (i.e. SMA) (OE.MAN.ALARM).

4.5.12 A.SELF.TEST

(1) The periodic self testing of the TOE are initiated from the OTA application (OE.SELF.TEST).

4.5.13 A.PHYSICAL

(1) The VCS including the TOE must be installed accordingly to the installation guidelines (NOE.INSTALL). Only authorised persons shall be given physical access to the VCS (NOE.ACCESS.CTRL). The TOE must be installed in a physical protected area, minimum approved for the highest security level of information handled in the system (NOE.PHYS.PROT).

4.5.14 A.TRAINING

(1) All users of VCS are fully trained to use, handle and interpret the VCS equipment (NOE.CCI), (NOE.USER.TRAIN), (NOE.MAN.TRAIN). The technicians should be trained to install the VCS including the TOE accordingly to the installation guidelines (NOE.INSTALL).

4.5.15 A.CLEARANCE

(1) Only authorised persons shall be given physical access to the VCS (NOE.ACCESS.CTRL). All OCP users have the minimum clearance for the maximum-security level of information handled in the system (NOE.CLEARANCE).

4.5.16 A.MAN.AUTHORISED

(1) Special authorisation is required to grant access to handle configuration and management of the VCS (OE.MAN.ACCESS).

4.5.17 A.VCS.COM / A.USAGE

(1) The VCS including the TOE must be installed accordingly to the installation guidelines (NOE.INSTALL).

4.5.18 A.AUDIT

(1) All audit data is stored on a secure way and authorised users ensures that the logs are maintained and inspected on a regular basis, and ensures that proper action is taken on any breaches of security (OE.AUDIT), (NOE.AUDIT). The audit functionality is put outside the TOE (NOE.INSTALL).

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

(1) The following explicit components have been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

5.1 Explicit Functional Components

Explicit Component	Identifier	Rationale
NONE		

6. SECURITY REQUIREMENTS

6.1 General

(1) This section contains the functional requirements that are provided by the TOE and the IT environment. These requirements consist of functional components from Part 2 of the Common Criteria (CC), extended with explicitly stated requirements.

6.2 TOE Security Functional Requirements

6.2.1 Functional components list

(1) The Table 6-1 lists the functional components included in this ST.

Component	Name
FAU_ARP.1(1)	Security alarms
FAU_ARP.1(2)	Security alarms
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_IFF.6	Illicit information flow monitoring
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_TST.1	TSF self test
FTP_TRP.1	Trusted path

Table 6-1 TOE Security Functional Requirements

6.2.2 Security audit

(1) This section involves recognising, recording and storing information related to security relevant activities.

FAU_ARP.1(1)	**Security alarms**
FAU_ARP.1.1(1)	The TSF shall take [*an action to raise a local alarm*] upon detection of a potential security violation.
	Dependencies: FAU_SAA.1 Potential violation analysis. Ref. table 6-5.
FAU_ARP.1(2)	**Security alarms**
FAU_ARP.1.1(2)	The TSF shall take [*an action to raise an alarm to the OTA application in order to send an alarm message to the management system (i.e. SMA)*] upon detection of a potential security violation.
	Dependencies: FAU_SAA.1 Potential violation analysis. Ref. table 6-5.

6.2.3 User data protection

(1) This section specifies the User Data Protection security requirements for the TOE.

FDP_IFC.2	**Complete Information Flow Control**
FDP_IFC.2.1	The TSF shall enforce the [*information flow control SFP*] on [*the following subjects:* • *TOE secure domain functions and* • *TOE non-secure domain functions* *for the following information:* • *potentially classified information (secure information) and* • *unclassified information (non-secure information)*] and all operations that cause that information to flow to and from subjects covered by the SFP. Note: The TOE information flow control SFP includes the policy statement to reject unacceptable messages attempted transmitted from the secure domain to the non-secure domain.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by the information flow control SFP.
	Dependencies: FDP_IFF.1 Simple security attributes is included.

FDP_IFF.1	**Simple security attributes**
FDP_IFF.1.1	The TSF shall enforce the [*information flow control SFP*] based on the following types of subject and information security attributes: [*The subjects are identified as blocks in the information flow block diagram, which is a part of the Information flow control SFP. The Information flow shall be controlled by the transmission security status.*].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*The rules are specified in the information flow control SFP*].
FDP_IFF.1.3	The TSF shall enforce [*no additional information flow control SFP rules*].
FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [*stated in the information flow control SFP*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [none].
	Dependencies: FDP_IFC.1 is covered as FDP_IFC.2 is included. FMT_MSA.3 is included.
FDP_IFF.6	**Illicit information flow monitoring**
FDP_IFF.6.1	The TSF shall enforce the [*information flow control SFP*] to monitor [*illicit information flows through the firewall*] when it exceeds the [*traffic thresholds (see Table 6-2)*].
	Dependencies: FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included.

6.2.4 Security management

(1) This section specifies the Security Management of the TOE.

FMT_MOF.1	**Management of security functions behaviour**
FMT_MOF.1.1	The TSF shall restrict the ability to [*determine the behaviour of*] the function [*security alarms*] to [*the role local configuration manager (see Table 6-2)*].
	Dependencies: FMT_SMR.1 Security roles. FMT_SMF.1 Specification of Management Functions.
FMT_MSA.1	**Management of security attributes**
FMT_MSA.1.1	The TSF shall enforce the [*none*] to restrict the ability to [*modify*] the security attributes [*shown in Table 6-2*] to [*the roles shown in the table*].

	Dependencies: FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included. FMT_SMR.1 Security roles. FMT_SMF.1 Specification of Management Functions.
FMT_MSA.2	**Secure security attributes**
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for [*security attributes*].
	Dependencies: FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included. FMT_MSA.1 Management of security attributes is included. FMT_SMR.1 Security roles.
FMT_MSA.3	**Static attribute initialization**
FMT_MSA.3.1	The TSF shall enforce the [*information flow control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the *SFP*.
FMT_MSA.3.2	The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.
	Dependencies: FMT_MSA.1 Management of security attributes is included. FMT_SMR.1 Security roles.

Security attribute	Role	Access
traffic_threshold If the traffic through the FW is higher than this threshold, an alarm is given to the management system.	Management system security manager	Read, write
TOE_mode The TOE can operate in the following modes: • Serving in a OCP, i.e. supporting voice services. A lamp panel is required (OTA in OCP) • Serving SMA, i.e. not supporting voice services. A lamp panel is not required (OTA for SMA).	Local configuration manager	Read, write
Transmission security status The status shall specify whether the microphone is connected to a non-secure channel.	OCP user	Read, write

Table 6-2 Management of user security attributes

6.2.5 Protection of the TOE Security Functions

(1) This section specifies the Protection of the TSF of the TOE.

FPT_FLS.1	**Failure with preservation of secure state**
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [*single point failures and security lamp failures*].
	Dependencies: No dependencies.
FPT_PHP.1	**Passive detection of physical attack**
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
	Dependencies: No dependencies.
FPT_TST.1	**TSF self test**
FPT_TST.1.1	The TSF shall run a suite of self tests [during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[none]] to demonstrate the correct operation of [the TSF].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [TSF data].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [TSF].
	Dependencies: No dependencies.

6.2.6 Trusted path/channels

(1) This section specifies the trusted path/channels of the TOE.

FTP_TRP.1	**Trusted Path**
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [*local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*]. (Note: OCP users are local users.)
FTP_TRP.1.2	The TSF shall permit [*the TSF, local users*] to initiate communication via the trusted path. (Note: OCP users are local users.)
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [[*OCP user audio handling and security indications*]].
	Dependencies: No dependencies.

6.3 TOE security assurance requirements

(1) The assurance level of the TOE is EAL5 augmented with ALC_FLR.3 Systematic flaw remediation. The assurance components are summarised in Table 6-3 below.

Assurance class	Assurance component name	Assurance family
ADV: Development	Security Architecture description	ADV_ARC.1
	Complete semi-formal functional specification with additional error information	ADV_FSP.5
	Implementation representation of the TSF	ADV_IMP.1
	Well-structured internals	ADV_INT.2
	Semi-formal modular design	ADV_TDS.4
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life Cycle Support	Production support, acceptance procedures and automation	ALC_CMC.4

	Development tools CM coverage	ALC_CMS.5
	Delivery procedures	ALC_DEL.1
	Identification of security measures	ALC_DVS.1
	Systematic flaw remediation	ALC_FLR.3
	Developer defined life-cycle model	ALC_LCD.1
	Compliance with implementation standards	ALC_TAT.2
ASE: Security Target Evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
Class ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: modular design	ATE_DPT.3
	Functional testing	ATE_FUN.1
	Independent testing – sample	ATE_IND.2
AVA: Vulnerability assessment	Methodical vulnerability analysis	AVA_VAN.4

Table 6-3 Security assurance requirements: EAL5

6.4 Security requirements rationale

6.4.1 Requirements are appropriate

(1) This table below identifies which SFRs satisfy which Objectives

Component / Objectives	FAU_ARP.1(1)	FAU_ARP.1(2)	FDP_IFC.2	FDP_IFF.1	FDP_IFF.6	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FPT_FLS.1	FPT_PHP.1	FPT_TST.1	FTP_TRP.1
O.ALARM.FAILURE	x	x											
O.ALARM.FW		x	x		x								
O.CROSS-TALK			x	x									
O.FILTER			x										
O.SEC.ATTRIBUTES				x		x	x	x	x				
O.SEC.NON-SEC	x	x	x							x		x	
O.SELF.TEST										x		x	
O.TX.STATUS			x	x									x
NO.SEALING											x		

Table 6-4: Mapping of Objectives to SFRs

(2) As it can be seen in Table 6-4 all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective.

6.4.1.1 Security Functional Requirements vs. Objectives

FAU_ARP.1(1) Security alarms

(1) The TOE will raise a local alarm indication if a TOE hardware or software failure is detected (O.ALARM.FAILURE). A failure that is reported may compromise the secure/non-secure protection (O.SEC.NON-SEC).

FAU_ARP.1(2) Security alarms

(2) The TOE will raise an alarm to the OTA application if a TOE hardware or software failure is detected (O.ALARM.FAILURE). The OTA application will if possible, transmit the alarm to the management system. The TOE will raise an alarm to the OTA application when the firewall traffic threshold is exceeded, a message is rejected in the firewall or the threshold value for generating alarm exceeds the maximum legal value (O.ALARM.FW). The OTA application will transmit the alarm to the management system. A failure that is reported may compromise the secure/non-secure protection (O.SEC.NON-SEC).

FDP_IFC.2 Complete information flow control

(3) The TOE has complete information flow control that controls all information flow. The information flow control prevents secure information to be transferred to non-secure channels (O.SEC.NON-SEC). Unacceptable acoustic cross-talk is prevented by blocking of audio devices (O.CROSS-TALK). The TOE gives correct security status, which prevents the user to talk classified on non-secure channels (O.TX.STATUS). The TOE filters all messages sent from the secure network to the non-secure network (O.FILTER) and will raise an alarm when a message is rejected (O.ALARM.FW)

FDP_IFF.1 Simple security attributes

(4) The transmission security status is a security attribute (O.SEC.ATTRIBUTES) that controls the information flow (O.TX.STATUS, O.CROSS-TALK).

FDP_IFF.6 Illicit information flow monitoring

(5) The illicit information flow monitoring will give an alarm if the traffic threshold is exceeded or a message is rejected in the firewall (O.ALARM.FW).

FMT_MOF.1 Management of security functions behaviour

(6) The TOE shall ensure that the TOE mode is an installation parameter (O.SEC.ATTRIBUTES).

FMT_MSA.1 Management of security attributes

(7) The validity of all security attributes received from the environment, are checked by the TOE (O.SEC.ATTRIBUTES).

FMT_MSA.2 Secure security attributes

(8) The TOE checks that the security attributes are secure (O.SEC.ATTRIBUTES).

FMT_MSA.3 Static attribute initialisation

(9) The default values for the firewall traffic threshold values shall be zero (O.SEC.ATTRIBUTES).

FPT_FLS.1 Failure with preservation of secure state

(10) The TOE is designed to fail in a safe manner. This includes security indicator failure, failure during self-test (O.SELF.TEST) and failure that compromises the secure/non-secure protection (O.SEC.NON-SEC).

FPT_PHP.1 Passive detection of physical attack

(11) The TOE has sealing (NO.SEALING) to protect the TOE against tampering.

FPT_TST.1 TSF Self Test

(12) Security critical functions will be tested by a combination of power-up tests, periodic tests, and/or continuous tests (O.SELF.TEST). A failure detected during this test, may compromise the secure/non-secure protection (O.SEC.NON-SEC).

FTP_TRP.1 Trusted path

(13) The TOE gives the OCP user an unambiguous indication of whether the microphone is connected to a non-secure channel (O.TX.STATUS).

6.4.2 Security dependencies are satisfied

(1) The table below shows a mapping of Functional Components to their dependencies.

Functional Component	Dependency	Included	Comments
TOE Security Functional Requirements			
FAU_ARP.1(1)	FAU_SAA.1	NO	Note 2) below
FAU_ARP.1(2)	FAU_SAA.1	NO	Note 2) below
FDP_IFC.2	FDP_IFF.1	YES	
FDP_IFF.1	FDP_IFC.1	YES	Note 1) below
	FMT MSA.3	YES	
FDP_IFF.6	FDP_IFC.1	YES	Note 1) below
FMT_MOF.1	FMT_SMR.1	NO	Note 3) below
	FMT_SMF.1	NO	Note 4) below
FMT_MSA.1	FDP_IFC.1	YES	Note 1) below
	FMT_SMF.1	NO	Note 4) below
	FMT_SMR.1	NO	Note 3) below
FMT_MSA.2	FDP_IFC.1	YES	Note 1) below
	FMT_MSA.1	YES	
	FMT_SMR.1	NO	Note 3) below
FMT_MSA.3	FMT_MSA.1	YES	
	FMT_SMR.1	NO	Note 3) below
FPT_FLS.1	None		
FPT_PHP.1	None		
FPT_TST.1	None		
FTP_TRP.1	None		

Table 6-5: Security Requirements dependencies

Note 1: FDP_IFF.1, FDP_IFF.6, FMT_MSA.1 and FMT_MSA.2 have a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

Note 2: FAU_ARP.1(1) and FAU_ARP.1(2) have a dependency to FAU_SAA.1 which is not included as it is part of the OTA application SW, ref. ch. 1.6.1.

Note 3: FMT_MOF.1, FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 have a dependency to FMT_SMR.1 which is not included as it is part of the OTA application SW, ref. ch. 1.6.1.

Note 4: FMT_MOF.1 and FMT_MSA.1 have a dependency to FMT_SMF.1 which is not included as it is part of the OTA application SW, ref. ch. 1.6.1.

6.4.3 SAR rationale

The SARs specified in this ST are according to EAL5.

7. TOE SUMMARY SPECIFICATION

7.1 TOE security functions

(1) This describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in chapter 6.2.

7.1.1 Security functions list

This chapter is left blank intentionally.

7.1.2 SF.Security.Alarm

(1) The TOE will raise an alarm to the OTA application (required non-TOE SW) in the following situations:

(a) The traffic through the FW exceeds the threshold value.

(b) The traffic drops below the threshold value.

(c) The threshold value for generating alarm is changed.

(d) The threshold value for generating alarm in the FW exceeds the maximum legal value.

(e) A message is rejected by the FW.

(2) The TOE forwards the alarm to the OTA application (required non-TOE SW) which will transmit the alarm to the management system.

(3) The TOE will raise a local alarm indication, and raise an alarm to the OTA application (required non-TOE SW) in the following situations:

(a) A firewall test failure is detected in the TOE.

(b) A hardware or software failure is detected in the TOE.

(4) The TOE forwards the alarm to the OTA application (required non-TOE SW), which will, if possible, transmit the alarm to the management system.

(5) Alarms are time-stamped by the management system.

7.1.3 SF.Information.Flow.Control

(1) The information flow control provides flow control between the user interfaces and the secure and non-secure network and information flow control between the secure and non-secure network. The flow control rules are based on:

(a) All messages from the secure network to the non-secure network are filtered in a firewall. If a message is rejected by the FW or the traffic through the FW exceeds the threshold value an alarm is generated.

(b) When there is a possibility that non-secure microphones may pick up from secure sources, the audio handling on the TOE will block secure audio to the audio devices.

(c) The TOE will prevent the microphones to be connected to the non-secure network in the case of a failing TOE security indicator.

7.1.4 SF.Security.Management

(1) The TOE can receive the following security management information:

(a) The mode the TOE shall operate in after a restart (installation parameter).

(b) The firewall traffic thresholds.

(2) If the threshold value exceeds the maximum legal value an alarm is generated.

7.1.5 SF.Self.Test

(1) The testing of TOE will detect errors in the security critical functions on the TOE and it will detect lamp errors. If a firewall failure or a hardware or software failure is detected in the TOE, an alarm is generated.

7.1.6 SF.Fail.Secure

(1) The most serious violation of the TSF is that classified voice or data on the secure network is sent on the non-secure network. The following measures shall prevent this to happen as a result of TOE-failures:

(a) The TOE is designed to handle single failures without violating the trusted functionality. In other words: If TOE fails, it will fail in a safe manner.

(b) The audio part of TOE is designed in such a way that the trusted functionality in TOE do not rely on any other modules. E.g. a failure may occur which implies that a security status given by the MFT application software in the workstation is corrupted on its way to the TOE. This should however not violate the security policy as the TOE informs the OCP user directly of whether the microphone is connected to a secure or a non-secure channel.

(c) If a security lamp failure is detected, the TOE will block the signals from the microphone to the non-secure voice path and an alarm is generated.

7.1.7 SF.Passive.Protection

(1) The TOE has a physical sealing.

7.1.8 SF.Trusted.Path

(1) The TOE provides a trusted path between itself and the OCP user for audio handling and for security related lamps.

7.2 TOE summary specification rationale

(1) The table below shows how TOE Security Functions satisfy SFRs.

TOE Security functions	SFRs	Description
SF.Security.Alarm	FAU_ARP.1(1), FAU_ARP.1(2)	The TOE security alarm function will raise security alarms automatically upon a potential security violation detected by the TOE firewall (FAU_ARP.1(2)), and upon detection of a failure in the TOE (FAU_ARP.1(1)).
SF.Information.Flow.Control	FDP_IFC.2, FDP_IFF.1, FDP_IFF.6	The TOE information flow control controls all information flows (FDP_IFC.2) determined by the transmission security status (FDP_IFF.1) and monitors possible misuse of the channel in the TOE firewall (FDP_IFF.6).
SF.Security.Management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3	The TOE security management function has a mode of operation as installation parameter (FMT_MOF.1) and receives firewall traffic threshold from the management system (FMT_MSA.1). These values are validated (FMT_MSA.2) and the default values are restrictive (FMT_MSA.3).
SF.Fail.Secure	FPT_FLS.1	The fail secure function preserves a secure state after failure.
SF.Passive.Protection	FPT_PHP.1	The TOE sealing is constructed so that physical tampering is easily discovered.
SF.Self.Test	FPT_TST.1	The TOE self-test function performs an underlying testing of the TOE.
SF.Trusted.Path	FTP_TRP.1	The TOE has trusted path/channels to the OCP user to ensure that the OCP user unambiguously is made aware whether the microphone is connected to a non-secure channel. The microphone is directly connected to the TSF.

Table 7-1: TOE Security Functions satisfy SFRs

(2) Strength of TOE security function analysis shall be performed on probabilistic or permutational functions.

(3) The TOE does not have any probabilistic or permutational functions. Hence, there are no TOE security functions having a TOE security function claim and there is no further strength of TOE security function analysis required.

8. NOTES

8.1 Acronyms and Abbreviations

CC	Common Criteria
CCI	Crypto/Comsec Controlled Item
DSP	Digital Signal Processor
EAL	Evaluation Assurance Level
FW	Firewall
G-A-G	Ground-Air-Ground
G-G	Ground-to-Ground
G-M-G	Ground-to-Maritime-Ground
HW	Hardware
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LOL	Loudspeaker and Lamps
MFT	Multifunction Terminal
NBC	Nuclear, Biological and Chemical
NSM	Nasjonal sikkerhetsmyndighet
OCP	Operator Controller Position
OPS	Operator Position Subsystem
OTA	Operator Terminal Adapter
PTT	Push To Talk
SFP	Security Function Policy
SFR	Security Functional Requirement(s)
SMA	Site Management Application
ST	Security Target
STT	Step To Talk
SW	Software
TGW	Telephone GateWay

TOE	Target of evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
VCS	Voice Communication System
VoIP	Voice over IP
VoX	Voice Operation Keying

8.2 Definitions

Classified information	Classified information is information regarded as sensitive by the security authorities for the owners of the system that comprises the TOE. Sensitive information is information that these security authorities determine must be protected because its unauthorised disclosure will cause perceivable damage.
Secure domain (red)	The domain that handles classified information in clear.
Non-secure domain (black)	The domain that does not handle classified information in clear.
Operator Controller Position (OCP)	The Operator Controller Position consists of one OTA, one MFT, one LOL, and audio accessories.