

OPERATOR TERMINAL ADAPTER SECURITY TARGET

Edition: **6.2.4**

19-September-11

Previous editions:

Ed. 6.2.3 08-June-10

Ed. 6.2.2 30-Oct-09

Ed. 6.2.1 28-Sep-09

Ed. 6.2 20-May-09

Ed. 6.1 14-jan-09

Author: **VIDAR KARLSEN**

Appr.: **PÅL TARALDSEN**

All pages in this document shall have the same edition number

TABLE OF CONTENTS

| | | |
|-----------|--|-----------|
| 1. | <u>SECURITY TARGET INTRODUCTION</u> | 4 |
| 1.1 | SECURITY TARGET IDENTIFICATION..... | 4 |
| 1.2 | SECURITY TARGET OVERVIEW | 4 |
| 1.3 | COMMON CRITERIA CONFORMANCE | 4 |
| 1.4 | RELATED DOCUMENTS..... | 5 |
| 1.5 | ABBREVIATIONS AND ACRONYMS | 5 |
| 1.6 | DEFINITIONS | 6 |
| 2. | <u>TOE DESCRIPTION</u> | 7 |
| 2.1 | OTA IN THE VCS..... | 7 |
| 2.2 | DEFINITION OF TOE PERIMETER | 7 |
| 2.3 | THE TOE HW | 8 |
| 2.4 | THE OTA APPLICATION SW | 9 |
| 2.5 | THE TOE SW | 10 |
| 2.6 | VOICE RECEPTION..... | 10 |
| 2.7 | VOICE TRANSMISSION | 11 |
| 2.8 | AUDIO DEVICES HW | 12 |
| 2.9 | OCP..... | 13 |
| 2.10 | SCOPE OF EVALUATION..... | 14 |
| 3. | <u>TOE SECURITY ENVIRONMENT</u> | 15 |
| 3.1 | ASSUMPTIONS..... | 15 |
| 3.2 | THREATS | 15 |
| 3.2.1 | IDENTIFICATION OF ASSETS..... | 15 |
| 3.2.2 | IDENTIFICATION OF THREAT AGENTS..... | 16 |
| 3.2.3 | THREATS | 16 |
| 3.3 | ORGANISATIONAL SECURITY POLICIES..... | 18 |
| 4. | <u>SECURITY OBJECTIVES</u> | 20 |
| 4.1 | TOE IT SECURITY OBJECTIVES..... | 20 |
| 4.2 | TOE NON-IT SECURITY OBJECTIVES..... | 21 |
| 4.3 | ENVIRONMENT IT SECURITY OBJECTIVES | 21 |
| 4.4 | ENVIRONMENT NON-IT SECURITY OBJECTIVES..... | 21 |
| 5. | <u>SECURITY REQUIREMENTS</u> | 23 |
| 5.1 | TOE SECURITY FUNCTIONAL REQUIREMENTS..... | 23 |
| 5.1.1 | SECURITY AUDIT..... | 23 |
| 5.1.2 | USER DATA PROTECTION | 24 |

| | | |
|------------|--|------------------|
| 5.1.3 | SECURITY MANAGEMENT | 25 |
| 5.1.4 | PROTECTION OF THE TSF | 26 |
| 5.1.5 | TRUSTED PATH/CHANNELS..... | 27 |
| 5.2 | SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT | 27 |
| 5.2.1 | SECURITY AUDIT | 27 |
| 5.2.2 | IDENTIFICATION AND AUTHENTICATION | 29 |
| 5.2.3 | SECURITY MANAGEMENT | 29 |
| 5.2.4 | PROTECTION OF THE TSF | 29 |
| 5.2.5 | PROTECTION OF THE IT ENVIRONMENT..... | 30 |
| 5.3 | TOE SECURITY ASSURANCE REQUIREMENTS..... | 31 |
| 5.4 | STRENGTH OF FUNCTION CLAIM..... | 31 |
| 6. | <u>TOE SUMMARY SPECIFICATION</u> | <u>32</u> |
| 6.1 | TOE SECURITY FUNCTIONS | 32 |
| 6.1.1 | SF.SECURITY.ALARM..... | 32 |
| 6.1.2 | SF.INFORMATION.FLOW.CONTROL | 32 |
| 6.1.3 | SF.SECURITY.MANAGEMENT | 32 |
| 6.1.4 | SF.SELF.TEST | 33 |
| 6.1.5 | SF.FAIL.SECURE | 33 |
| 6.1.6 | SF.PASSIVE.PROTECTION | 33 |
| 6.1.7 | SF.DOMAIN.SEPARATION..... | 33 |
| 6.1.8 | SF.TRUSTED.PATH..... | 34 |
| 6.2 | ASSURANCE MEASURES | 35 |
| 7. | <u>PROTECTION PROFILES CLAIMS</u> | <u>37</u> |
| 8. | <u>RATIONALE</u> | <u>38</u> |
| 8.1 | INTRODUCTION..... | 38 |
| 8.2 | SECURITY OBJECTIVES FOR THE TOE RATIONALE | 38 |
| 8.3 | SECURITY REQUIREMENTS RATIONALE..... | 41 |
| 8.3.1 | REQUIREMENTS ARE APPROPRIATE | 41 |
| 8.3.1.1 | Security Functional Requirements vs. Objectives..... | 41 |
| 8.3.1.2 | Objectives vs. Security Functional Requirements..... | 42 |
| 8.3.2 | ENVIRONMENT REQUIREMENTS ARE APPROPRIATE | 45 |
| 8.3.2.1 | Environment IT Security Objectives vs. Security Requirements for the IT Environment..... | 45 |
| 8.3.3 | SECURITY DEPENDENCIES ARE SATISFIED..... | 46 |
| 8.4 | TOE SUMMARY SPECIFICATION RATIONALE | 47 |
| 9. | <u>CHANGES</u> | <u>48</u> |

1. SECURITY TARGET INTRODUCTION

1.1 Security Target identification

| | |
|--|--|
| Title | Security Target for Operator Terminal Adapter (OTA) |
| Target of evaluation (TOE) Identification | <p>The TOE comprises the following OTA modules:</p> <ul style="list-style-type: none"> • OTA hardware: 3AQ 21564 AAAA ICS5A, ICS7, ICS7A, ICS7B • OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.2 <p>- and one out the following customer specific variants of the OTA firewall definition file:</p> <ul style="list-style-type: none"> • 3AQ 24862 EAAA Version 6.2.2 (certificate baseline), or • 3AQ 24862 HAAA Version 6.2.2, or • 3AQ 24862 TRAA Version 6.2.7 <p>The list of document editions associated with the certificate baseline versions is given in ref. [5].</p> <p>Note: the version of the OTA trusted kernel is incremented from version 6.2.1 to version 6.2.2 due to a security flaw remediation.</p> |
| Assurance level | EAL5 augmented with ALC_FLR.3 (Systematic flaw remediation) |

1.2 Security Target overview

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.

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.

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.

1.3 Common Criteria conformance

This TOE and ST are consistent with the following specifications:

- The OTA has been developed to include components as defined in the Common Criteria (CC) version 2.3 part 2 [2].

- The OTA has been developed to conform to the EAL5 assurance level augmented with ALC_FLR.3, as identified in the Common Criteria version 2.3 part 3 [3].

1.4 Related documents

| | | |
|-----|-------------------------------|--|
| [1] | 3AQ 24863 AAAA DEZZA | OTA Security Design |
| [2] | CCMB-2005-08-002 | Common Criteria version 2.3 part 2 |
| [3] | CCMB-2005-08-003 | Common Criteria version 2.3 part 3 |
| [4] | C-M(55)15(Final), Enclosure C | Security within the North Atlantic Treaty Organisation |
| [5] | 3AQ 24863 AAAA DSL | Document Status List for OTA Security Evaluation |

1.5 Abbreviations and acronyms

| | |
|-------|------------------------------------|
| ANS | Access Network Subsystem |
| 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 |
| GWS | GateWay Subsystem |
| 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 |
| RDS | Radio Distribution Subsystem |
| RES | Radio Equipment Subsystem |
| RGW | Radio GateWay |
| SF | Security Function |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement(s) |
| SMA | Site Management Application |
| SOF | Strength of Function |
| 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 |
| TSP | TOE Security Policy |
| VCS | Voice Communication System |

| | |
|------|---------------------------|
| VMS | VCS Management Subsystem |
| VoIP | Voice over IP |
| VoX | Voice Operation Keying |
| VRS | Voice Recording Subsystem |

1.6 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. |

2. TOE DESCRIPTION

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.

2.1 OTA in the VCS

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

- OTA in OCP (in the Operator Position Subsystem in the figure)
- OTA for SMA (in the Access Network Subsystem in the figure)

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.

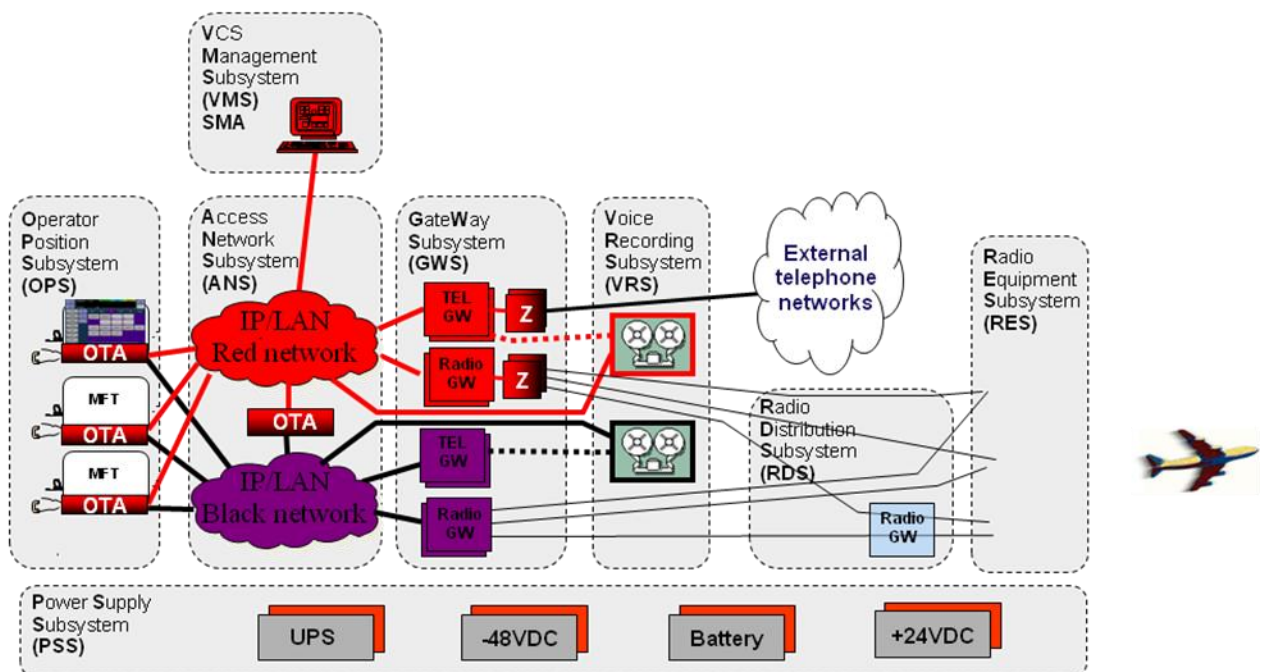


Figure 1 VCS architecture

2.2 Definition of TOE perimeter

The TOE is the parts of the OTA implementing the core security functions, which must be highly trusted. The TOE is defined in section 1.1 "Security Target identification" and comprises:

- The complete OTA HW; and
- One software configuration item comprising a defined set of OTA software modules.

The TOE software consists of:

- The firewall including drivers;

- Boot software and software loader; and
- The red/black separation software including task switching; and
- DSP Sw

The OTA application software is running in the secure and non-secure software tasks as illustrated in Figure 2 showing the OTA architecture. The OTA application software is considered less security critical and is outside the TOE.

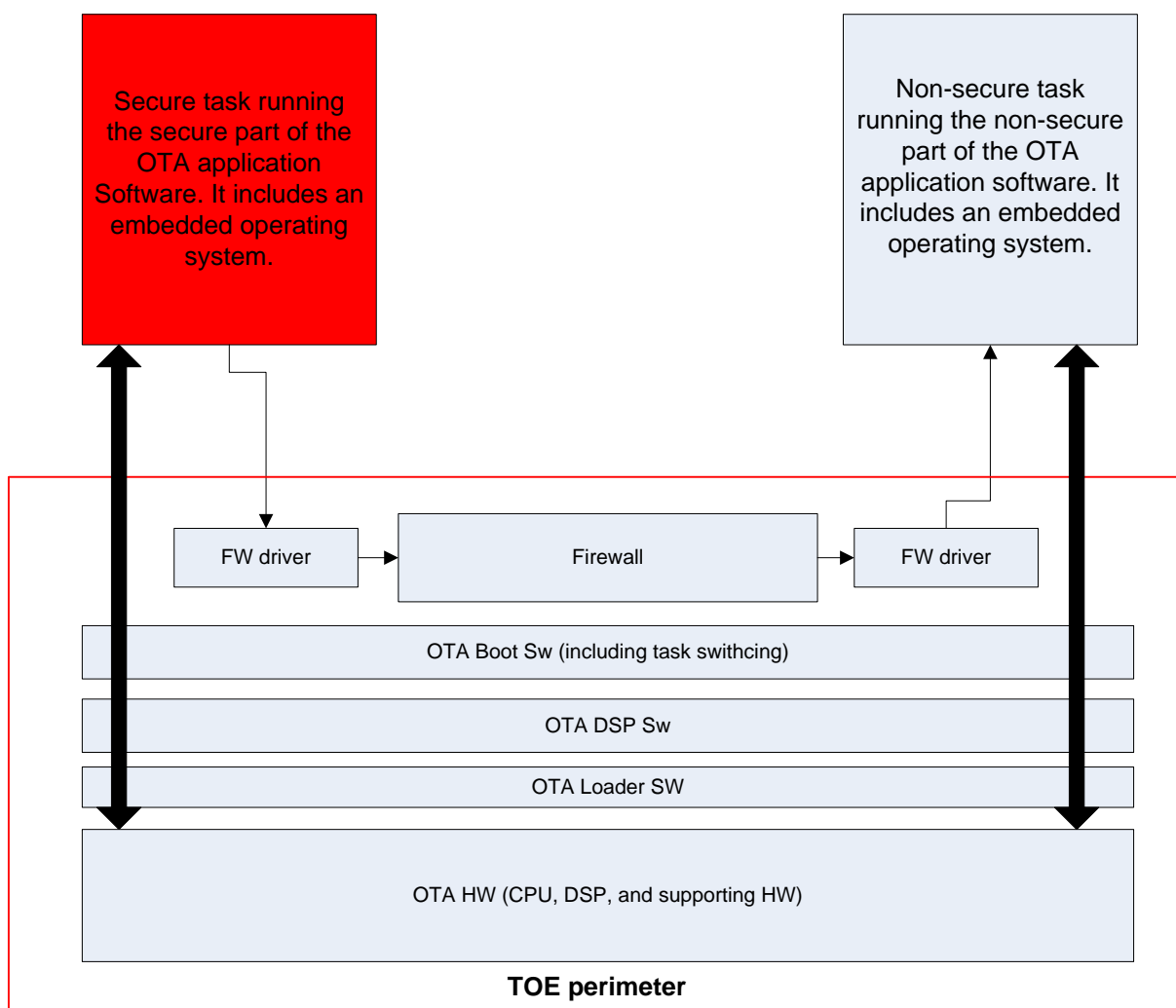


Figure 2 OTA architecture

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

2.3 The TOE HW

The TOE HW provides connection for the audio devices, the loudspeaker and lamps and the Ethernet interfaces, see figure 3 below.

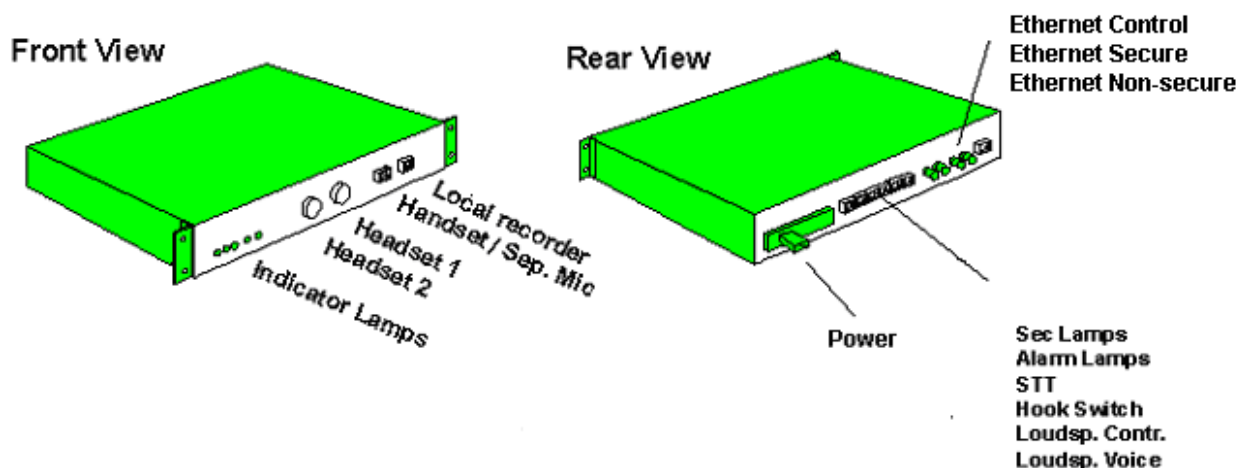


Figure 3 TOE mechanical characteristics

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.

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

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.

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.

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 3).

2.4 The OTA application SW

The OTA application SW performs the following main functions:

- **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 chapter 2.6 and 2.7 below.
- **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.

- 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).

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.

2.5 The TOE SW

The TOE SW as defined in section 1.1 performs the following main functions:

- Firewall
 - The firewall checks all messages from secure to non-secure domain and accepts messages compliant with the firewall configuration file.
 - The firewall configuration file is customized at compile time according to operational needs
- 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.
- SW loader, HW initialisation, self-tests, start-up and task switching functions.
- DSP with echo cancelling and VoX functions.

2.6 Voice reception

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

- The radio communication service provides connections from the Radio Gateway
- The telephone communication service provides connection from the TGW
- The intercom communication service provides connections from other OCPs
- The loop monitoring communication service provides connections from the TGW

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

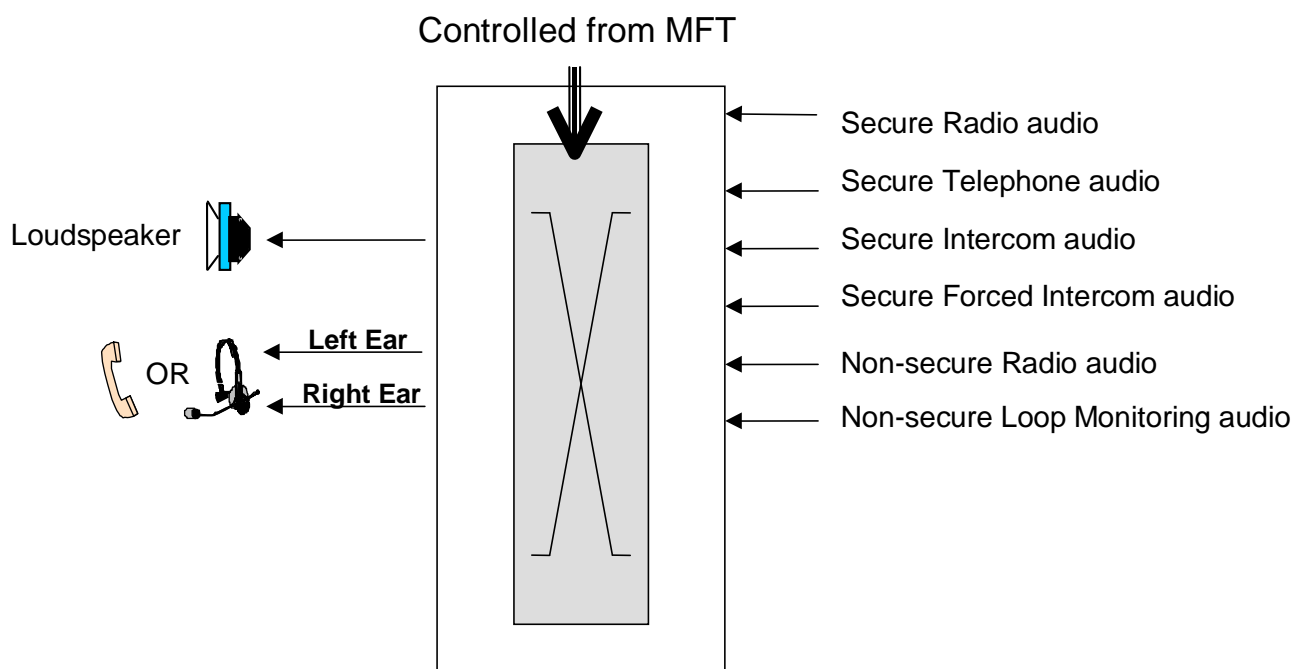


Figure 4 Audio presentation capabilities

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.

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

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.

2.7 Voice transmission

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

- The radio communication service provides connection to the Radio Gateway
- The telephone communication service provides connection to the TGW
- 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

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.

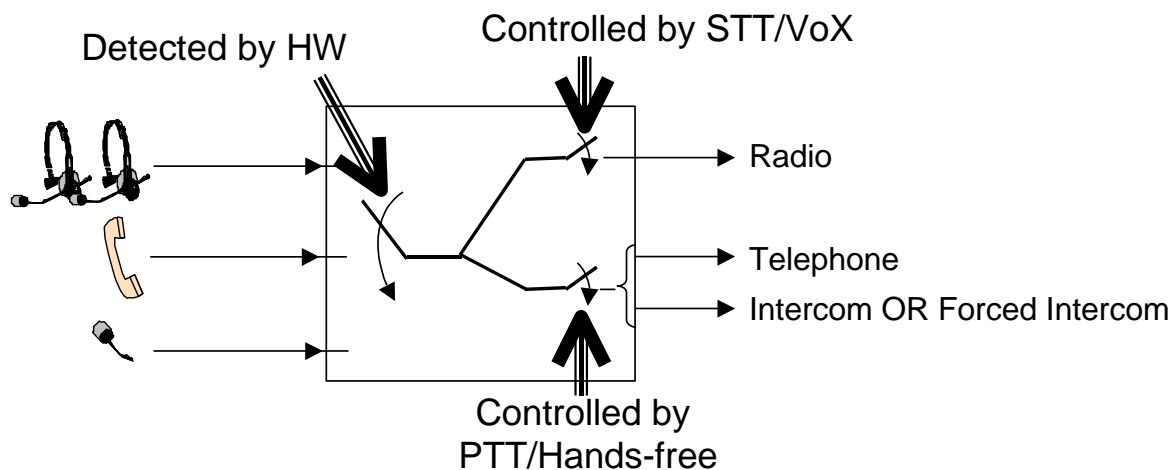


Figure 5 Audio transmission capabilities

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 5:

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.

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.

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

2.8 Audio devices HW

The audio devices of the OCP position are identified in Figure 6 below.

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.

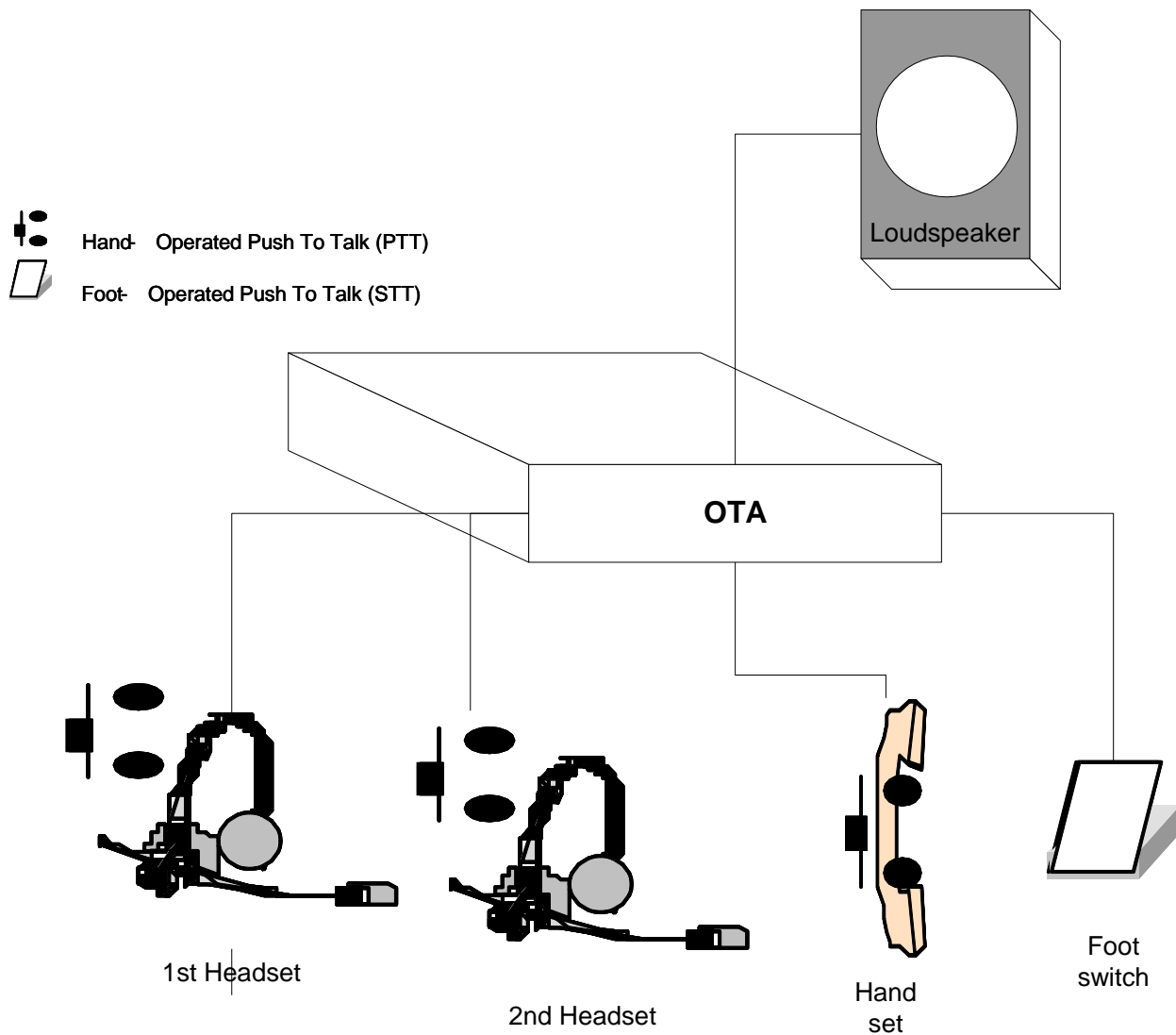


Figure 6 Audio devices

2.9 OCP

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.

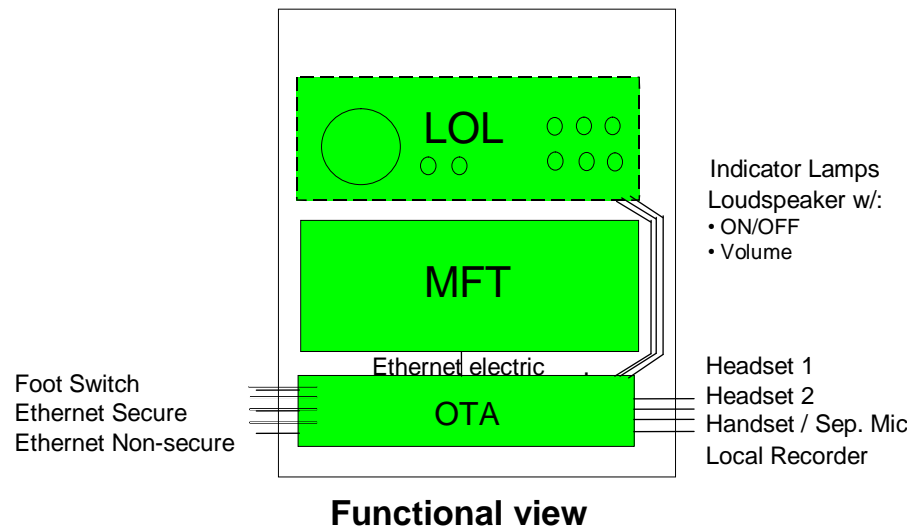


Figure 7 OCP

2.10 Scope of evaluation

- The TOE is the parts of the OTA as identified in section 1.1 "Security Target identification"
- The scope of evaluation is evaluation of security functions in the TOE. These security functions are identified in section 6.1 "TOE security functions".

The TEMPEST certification is not within this scope of evaluation.

3. TOE SECURITY ENVIRONMENT

This section provides the statement of the TOE security environment, which identifies and explains all:

1. Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.
2. Known and presumed threats countered by either the TOE or by the security environment.
3. Organisational security policies the TOE must comply with.

3.1 Assumptions

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. |

3.2 Threats

This section identifies the assets, threat agents and threats.

3.2.1 Identification of Assets

The assets within the TOE that needs protection are all classified information transmitted through the TOE.

3.2.2 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. |

3.2.3 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 | <ol style="list-style-type: none"> 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. |

3.3 Organisational security policies

The TOE must be compliant with:

- Audio coupling of secure communications onto active non-secure lines at operator consoles shall be avoided i.a.w. C-M(55)15(Final) [4], Enclosure C, paragraphs 72 and 74.

4. SECURITY OBJECTIVES

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 (environment) 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 (environment) in order to send an alarm message to the management system.

O.ALARM.FW The TOE shall raise an alarm to the OTA application (environment) 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.

5. SECURITY REQUIREMENTS

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.

5.1 TOE Security Functional Requirements

The Table 1 list 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_AMT.1 | Abstract machine testing |
| FPT_FLS.1 | Failure with preservation of secure state |
| FPT_PHP.1 | Passive detection of physical attack |
| FPT_SEP.1 | TSF domain separation |
| FTP_TRP.1 | Trusted path |

Table 1 TOE Security Functional Requirements

5.1.1 Security Audit

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 is included.

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 is included.

5.1.2 User Data Protection

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 provide *[no list of additional SFP capabilities]*.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: *[stated in the information flow control SFP]*.

FDP_IFF.1.6 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 the [*illicit information flows through the firewall*] when it exceeds the [*traffic thresholds (see table 2)*].

Dependencies: AVA_CCA.1 Covert channel analysis is included.
FDP_IFC.1 Subset information flow control is covered as
FDP_IFC.2 is included.

5.1.3 Security Management

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 2)*].

Dependencies: FMT_SMR.1 Security roles is included.

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 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 is included.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model is included.
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 is included.

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 is included.

| 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: <ul style="list-style-type: none"> 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 2: Management of user security attributes

5.1.4 Protection of the TSF

This section specifies the Protection of the TSF of the TOE.

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests [*during initial start-up, periodically during normal operation*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

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: ADV_SPM.1 Informal TOE security policy model is included.

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: FMT_MOF.1 Management of security functions behavior is included.

FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5 Trusted path/channels

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 the following [*local*] users that is logical distinct from the other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

(Note: OCP users are local users.)

FTP_TRP.1.2 The TSF shall permit [*the TSF and the local users identified in FTP_TRP.1.1*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*OCP user audio handling and security indications*].

5.2 Security requirements for the IT environment

This section details the IT security requirements to be met by the IT environment of the TOE. Table 3 lists the IT security requirements to be provided by the IT environment.

| Component | Name |
|---------------|-------------------------------|
| FAU_ARP.1.Env | Security alarms |
| FAU_GEN.1 | Audit data generation |
| FAU_SAA.1 | Potential violation analysis |
| FAU_SAR.1 | Audit review |
| FAU_STG.1 | Protected audit trail storage |
| FIA_UAU.1 | Timing of authentication |
| FIA_UID.1 | Timing of identification |
| FMT_SMR.1 | Security roles |
| THA_REQ.1.Env | Abstract machine testing |
| FPT_STM.1 | Reliable time stamps |

Table 3 Security requirements for the IT environment

5.2.1 Security audit

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

FAU_ARP.1.Env

Security alarms

FAU_ARP.1.1

The IT environment shall take [*an action to send an alarm to the management operator*] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis is included.

FAU_GEN.1

Audit Data Generation

FAU_GEN.1.1

The IT environment shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions
- b) All auditable events for the [*not specified*] level of audit; and
- c) [*Firewall traffic threshold alarm, Change of Firewall alarm threshold, Firewall traffic rejection alarm, Firewall testing alarm, Hardware and software failure alarm*].

FAU_GEN.1.2

The IT environment shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

Dependencies: FPT_STM.1 Reliable time stamps is included.

FAU_SAA.1

Potential violation analysis

FAU_SAA.1.1

The IT environment shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation in the TSP.

FAU_SAA.1.2

The IT environment shall enforce the following rules for monitoring audited events:

- a) Accumulation or combination of [*none*] known to indicate a potential security violation.
- b) [*None*]

Dependencies: FAU_GEN.1 Audit data generation is included.

FAU_SAR.1

Audit Review

FAU_SAR.1.1

The IT environment shall provide [*authorised users*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

The IT environment shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation is included.

FAU_STG.1

Protected Audit Trail Storage

FAU_STG.1.1

The IT environment shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The IT environment shall be able to [*prevent*] modifications to the audit records.

Dependencies: FAU_GEN.1 Audit data generation is included.

5.2.2 Identification and authentication

FIA_UAU.1

Timing of authentication

FIA_UAU.1.1

The IT environment shall allow [*change of transmission security status and mode of operation*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The IT environment shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification is included.

FIA_UID.1

Timing of identification

FIA_UID.1.1

The IT environment shall allow [*change of transmission security status and mode of operation*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The IT environment shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.3 Security Management

FMT_SMR.1

Security roles

FMT_SMR.1.1

The IT environment shall maintain the roles [*OCP user, management system security operator and local configuration manager*].

FMT_SMR.1.2

The IT environment shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification is included.

5.2.4 Protection of the TSF

THA_REQ.1.Env

Abstract machine testing

THA_REQ.1

The OTA applications shall initiate the test of the firewall in the TOE [*periodically during normal operation*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Note: The OTA application triggers the test of the firewall in the TOE. However, the TOE detects if the test is not run periodically and will in that case raise a local alarm indication and halt operation.

5.2.5 Protection of the IT environment

FPT_STM.1 **Reliable time stamps**

FPT_STM.1.1 The IT environment shall be able to provide reliable time stamps for its own use.

5.3 TOE security assurance requirements

The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL5 level of assurance, augmented with ALC_FLR.3. The assurance components are summarised in Table 4 below.

| Assurance class | | Assurance components |
|-------------------------------------|-----------|--|
| Configuration Management | ACM_AUT.1 | Partial CM automation |
| | ACM_CAP.4 | Generation support and acceptance procedures |
| | ACM_SCP.3 | Development tools CM coverage |
| Class ADO: Delivery and operation | ADO_DEL.2 | Detection of modification |
| | ADO_IGS.1 | Installation, generation and start-up procedures |
| Class ADV: Development | ADV_FSP.3 | Semiformal functional specification |
| | ADV_HLD.3 | Semiformal high-level design |
| | ADV_IMP.2 | Implementation of the TSF |
| | ADV_INT.1 | Modularity |
| | ADV_LLD.1 | Descriptive low-level design |
| | ADV_RCR.2 | Semiformal correspondence demonstration |
| | ADV_SPM.3 | Formal TOE security policy model |
| Class AGD: Guidance documents | AGD_ADM.1 | Administrator guidance |
| | AGD_USR.1 | User guidance |
| Class ALC: Life Cycle support | ALC_DVS.1 | Identification of security measures |
| | ALC_FLR.3 | Systematic flaw remediation |
| | ALC_LCD.2 | Standardised life-cycle model |
| | ALC_TAT.2 | Compliance with implementation standards |
| Class ATE: Tests | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.2 | Testing: low level design |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing – sample |
| Class AVA: Vulnerability assessment | AVA_CCA.1 | Covert channel analysis |
| | AVA_MSU.2 | Validation of analysis |
| | AVA_SOF.1 | Strength of TOE security function evaluation |
| | AVA_VLA.3 | Moderately resistant |

Table 4 Assurance Requirements: EAL5

5.4 Strength of Function Claim

A Strength of Function (SOF) claim of SOF-high is made for the TOE. There are no TOE security functions having a TOE security function claim.

6. TOE SUMMARY SPECIFICATION

6.1 TOE security functions

This describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in chapter 5.1.

6.1.1 SF.Security.Alarm

The TOE will raise an alarm to the OTA application in the following situations:

- The traffic through the FW exceeds the threshold value.
- The traffic drops below the threshold value.
- The threshold value for generating alarm is changed.
- The threshold value for generating alarm in the FW exceeds the maximum legal value.
- A message is rejected by the FW.

The OTA application will transmit the alarm to the management system.

The TOE will raise a local alarm indication, and raise an alarm to the OTA application in the following situations:

- A firewall test failure is detected in the TOE.
- A hardware or software failure is detected in the TOE.

The OTA application, will if possible, transmit the alarm to the management system.

Alarms are time-stamped by the management system.

6.1.2 SF.Information.Flow.Control

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:

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

6.1.3 SF.Security.Management

The TOE can receive the following security management information:

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

- The firewall traffic thresholds.

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

6.1.4 SF.Self.Test

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.

6.1.5 SF.Fail.Secure

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:

- 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.
- 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.
- 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.

6.1.6 SF.Passive.Protection

The TOE has a physical sealing.

6.1.7 SF.Domain.Separation

The TOE establishes and maintains the following domains:

- Non-secure domain
- Secure domain
- Firewall domain

The firewall checks all messages from secure to non-secure domain.

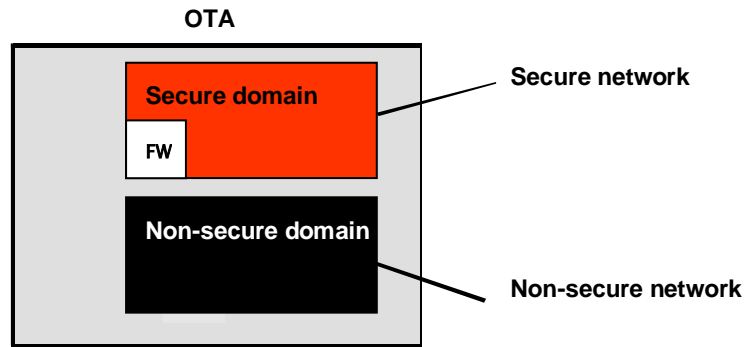


Figure 1 OTA Domains

6.1.8 SF.Trusted.Path

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

6.2 Assurance measures

Table 5 lists the assurance components defined by EAL5 augmented with ALC_FLR.3 and the documentation submitted as assurance measures.

| Assurance component | Component name | Assurance measure |
|---------------------|--|--|
| ACM_AUT.1 | Partial CM automation | 3aq 21530 OTA CM plan. |
| ACM_CAP.4 | Generation support and acceptance procedures | 3aq 21530 OTA CM plan. |
| ACM_SCP.3 | Development tools CM coverage | 3aq 21530 OTA CM plan. |
| ADO_DEL.2 | Detection of modification | PRO 2024 Deliver Products |
| ADO_IGS.1 | Installation, generation and start-up procedures | 3aq 12889 OTA Technical Manual. |
| ADV_FSP.3 | Semiformal functional specification | OTA Security Design [1]. |
| ADV_HLD.3 | Semiformal high-level design | OTA Security Design [1]. |
| ADV_IMP.2 | Implementation of the TSF | Various source code modules for the TSF, VHDL code for HW. |
| ADV_INT.1 | Modularity | OTA Security Design [1]. |
| ADV_LLD.1 | Descriptive low-level design | OTA Security Design [1]. |
| ADV_RCR.2 | Semiformal correspondence demonstration | OTA Security Design [1]. |
| ADV_SPM.3 | Formal TOE security policy model | OTA Security Design [1]. |
| AGD_ADM.1 | Administrator guidance | 3aq 12889 OTA Technical Manual. |
| AGD_USR.1 | User guidance | 3aq 22363 OCP Operator Manual. |
| ALC_DVS.1 | Identification of security measures | POL 0046 Ed. 14 Grunnlagsdokument for sikkerhet for Thales Norway AS (Thales Norway security regulations). |
| ALC_FLR.3 | Systematic flaw remediation | 3aq 21530 OTA CM plan, 3aq 12889 OTA Technical Manual |
| ALC_LCD.2 | Standardised life-cycle model | 3aq 21530 OTA CM plan |
| ALC_TAT.2 | Compliance with implementation standards | 3aq 21530 OTA CM plan, |

| | | |
|-----------|--|--|
| ATE_COV.2 | Analysis of coverage | OTA Security Design [1]. |
| ATE_DPT.2 | Testing: low level design | 3aq 21530 Integration test specification |
| ATE_FUN.1 | Functional testing | 3aq 21530 Integration test specification |
| ATE_IND.2 | Independent testing – sample | Performed at the TCN lab by an independent evaluation agency |
| AVA_CCA.1 | Covert channel analysis | OTA Security Design [1]. |
| AVA_MSU.2 | Validation of analysis | OTA Security Design [1]. |
| AVA_SOF.1 | Strength of TOE security function evaluation | OTA Security Target. |
| AVA_VLA.3 | Moderately resistant | OTA Security Design [1]. |

Table 5: Assurance measures

Ref. [5] is the document status list that includes the assurance measures listed in Table 5.

7. PROTECTION PROFILES CLAIMS

There are no Protection Profile Claims.

8. RATIONALE

8.1 Introduction

This section demonstrates that the TOE provides an effective set of IT security countermeasures within the security environment and that the TOE summary specification addresses the requirements.

8.2 Security Objectives for the TOE Rationale

| Threats/ Assumptions Objectives | 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 | | | | | | | | | | | |
| O.FILTER | | | x | | | | | | | | | | | | | | |
| O.SEC.ATTRIBUTES | | | x | | | | | x | | | | | | | | | |
| O.SEC.NON-SEC | x | | | | | | | | | | | | | | | | |
| O.SELF.TEST | x | | | x | | | | | | | | | | | | | |
| O.TX.STATUS | | | | | x | | | | | | | | | | | | |
| NO.SEALING | | x | | | | | | | | | | | | | | | |
| NO.TEMPEST | x | | | | | | x | | | | | | | | | | |
| OE.AUDIT | | | | | | | | | | | | | | | | | x |
| OE.MAN.ACCE | | | | | | | | 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 6 Mapping of Objectives to Threats and Assumptions

As can be seen from Table 6, 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.

T.CONN.SEC.NON-SEC

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.

T.TAMPERING

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).

T.MISUSE

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 covert 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 covert channels.

T.WRONG.SEC.IND

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).

T.SEC.IND.MISSING

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).

T.ACOUSTIC.PICK-UP

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).

T.TEMPEST

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).

T.UNAUTHORISED.USE

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).

A.OTA.ALARM

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

A.SELF.TEST

The periodic functions for abstract machine testing of the TOE are initiated from the OTA application (OE.SELF.TEST).

A.PHYSICAL

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).

A.TRAINING

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).

A.CLEARANCE

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).

A.MAN.AUTHORISED

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

A.VCS.COM / A.USAGE

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

A.AUDIT

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).

8.3 Security Requirements Rationale

8.3.1 Requirements are appropriate

Table 7 identifies which SFRs satisfy the Objectives in chapter 4.

| Component | 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_AMT.1 | FPT_FLS.1 | FPT_PHP.1 | FPT_SEP.1 | FTP_TRP.1 |
|------------------|--------------|--------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Objectives | | | | | | | | | | | | | | |
| O.ALARM.FAILURE | x | x | | | | | | | | | | | | |
| O.ALARM.FW | | x | x | | x | | | | | | | | | |
| O.CROSS-TALK | | | x | x | | | | | | | | | | |
| O.FILTER | | | x | | | | | | | | | | x | |
| O.SEC.ATTRIBUTES | | | | x | | x | x | x | x | | | | | |
| O.SEC.NON-SEC | x | x | x | | | | | | | x | x | | x | |
| O.SELF.TEST | | | | | | | | | | x | x | | | |
| O.TX.STATUS | | | x | x | | | | | | | | | | x |
| NO.SEALING | | | | | | | | | | | | x | | |

Table 7: Mapping of Objectives to SFRs

As it can be seen in Table 7 all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective. Therefore, as demonstrated in Table 6 and Table 7 all SFRs specified for the TOE are appropriate to counter the threats and meet the objectives of the TOE.

8.3.1.1 Security Functional Requirements vs. Objectives

FAU_ARP.1(1) Security alarms

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

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

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

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

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

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

FMT_MSA.1 Management of security attributes

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

FMT_MSA.2 Secure security attributes

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

FMT_MSA.3 Static attribute initialisation

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

FPT_AMT.1 Abstract machine testing

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).

FPT_FLS.1 Failure with preservation of secure state

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

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

FPT_SEP.1 TSF domain separation

To handle both secure and non-secure information (O.SEC.NON-SEC), the TOE has well defined division between the secure and non-secure domain. All message transferred from the secure network to the non-secure network is filtered in the firewall (O.FILTER).

FTP_TRP.1 Trusted path

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

8.3.1.2 Objectives vs. Security Functional Requirements

O.ALARM.FAILURE

The TOE will raise a local alarm indication FAU_ARP.1(1) and provides automatic alarm sending to the OTA application FAU_ARP.1(2), if a potential security violation is detected due to failure in the TOE. The OTA application will if possible, transmit the alarm to the management system.

O.ALARM.FW

FAU_ARP.1(2) provides automatic alarm sending to the OTA application, if a potential security violation is detected. The OTA application will if possible, transmit the alarm to the management system.

The TOE shall ensure that information transmitted from secure domain to non-secure domain is unclassified. This is handled by FDP_IFC.2 that provides the information flow control through the TOE and rejects attempts to send unacceptable messages transmitted in the direction from the secure domain to the non-secure domain. An alarm will be sent to the OTA application when a message is rejected. The OTA application will transmit the alarm to the management system.

FDP_IFF.6 provides monitoring of exploitation of covert channels in the TOE (i.e. through the firewall) and provides automatic alarm sending to the OTA application, if a potential security violation is detected (i.e. a traffic threshold is exceeded). The OTA application will transmit the alarm to the management system.

O.CROSS-TALK

The TOE shall control the information to/from the TOE audio interfaces to prevent unacceptable acoustic cross-talk. This is handled by FDP_IFC.2 that provides the information flow control through the TOE.

The information flow control rules are dependent of the transmission security status as handled by FDP_IFF.1.

O.FILTER

The TOE shall ensure that information transmitted from secure domain to non-secure domain is unclassified. This is handled by FDP_IFC.2 that provides the information flow control through the TOE.

FPT_SEP.1 provides separation of the TOE domains: secure domain and non-secure domain.

O.SEC.NON-SEC

FAU_ARP.1(1) will raise a local alarm indication if a potential security violation is detected due to failure in the TOE.

FAU_ARP.1(2) will provide automatic alarm sending to the management system, if a potential security violation is detected in the firewall.

FDP_IFC.2 provides the information flow control through the TOE that prevents information to flow from secure domain to non-secure domain except information that TOE as verified is unclassified.

FPT_AMT.1 provides that security critical functions are tested by a combination of power-up tests, periodic tests and/or continuous tests.

FPT_FLS.1 provides preservation of a secure state after a single point of failure and security indicator failure.

FPT_SEP.1 provides separation of the TOE domains: secure domain and non-secure domain.

O.SEC.ATTRIBUTES

The information flow control rules are dependent of the transmission security status as handled by FDP_IFF.1.

FMT_MOF.1 ensures that the TOE mode of operation is an installation parameter.

FMT_MSA.1 provides check validity on all security attributes received by the TOE.

FMT_MSA.2 provides that the security attributes are secure.

FMT_MSA.3 provides that the default values for the firewall traffic threshold are restrictive.

O.SELF.TEST

FPT_AMT.1 provides that security critical functions are tested by a combination of power-up tests, periodic tests and/or continuous tests.

FPT_FLS.1 provides preservation of a secure state after a single failure and security indicator failure.

O.TX.STATUS

FDP_IFC.2 provides the information flow control through the TOE. This information flow is controlled by the transmission security status.

FDP_IFF.1 provides the OCP user an unambiguous indication whether the microphone is connected to a non-secure channel using a trusted channel provided by FTP_TRP.1.

NO.SEALING

FPT_PHP.1 provides the passive protection of the TOE.

8.3.2 Environment requirements are appropriate

Table 8 identifies which Security requirements for the IT environment that satisfy the Objectives in chapter 4.

| Components | FAU_ARP.1.Env | FAU_GEN.1 | FAU_SAA.1 | FAU_SAR.1 | FAU_STG.1 | FIA_UAU.1 | FIA_UID.1 | FMT_SMR.1 | FPT_STM.1 | THA_REQ.1.Env |
|---------------------------|---------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|---------------|
| Environment IT Objectives | | | | | | | | | | |
| OE.AUDIT | | x | x | x | x | | | x | x | |
| OE.MAN.ACCESS | | | | | | x | x | x | | |
| OE.MAN.ALARM | x | | x | | | | | | | |
| OE.RECORDING | | x | | x | x | | | | x | |
| OE.SELF.TEST | | | | | | | | | | x |

Table 8: Mapping of Environment IT Objectives to Components

As it can be seen in Table 8, all objectives are satisfied by at least one Security requirement for the IT environment and all Security requirements for the IT environment are required to meet at least one Environment IT Objectives.

8.3.2.1 Environment IT Security Objectives vs. Security Requirements for the IT Environment

OE.AUDIT

The management system shall receive auditable events indicating type of event and outcome of the event from the TOE and store them with timestamp (FPT_STM.1) and TOE identity (FAU_GEN.1). All auditable events that are defined as security related events are recognised by the management system (FAU_SAA.1). The management system shall protect the stored audit records from unauthorised deletion and prevent modifications (FAU_STG.1). Authorised management system security operators (FMT_SMR.1) can read the stored event records (FAU_SAR.1).

OE.MAN.ACCESS

Management operators must identify themselves (FIA_UID.1) and authenticate themselves (FIA_UAU.1) before they can perform management and configuration and manage audit records as determined by their role (FMT_SMR.1).

OE.MAN.ALARM

The management system shall raise an alarm (FAU_ARP.1.Env) upon reception of an alarm or auditable event from the OTA application that potentially can indicate a security violation (FAU_SAA.1).

OE.RECORDING

The IT environment shall receive audio to be recorded from the TOE and store it with timestamp (FPT_STM.1) and information that can be used to uniquely identify the OCP and the OCP user (FAU_GEN.1). The recorded voice shall be protected for a specified period against modification (FAU_STG.1). It shall be possible to replay the voice recorded (FAU_SAR.1) from a given OCP.

OE.SELF.TEST

The OTA application provides that the firewall test in the TOE are tested by periodic tests (THA_REQ.1.Env).

8.3.3 Security dependencies are satisfied

Table 9 shows a mapping of Functional Components to their dependencies.

| Functional Component | Dependency | Included |
|---|-------------|----------|
| <u>TOE Security Functional Requirements</u> | | |
| FAU_ARP.1(1) | FAU_SAA.1 | YES |
| FAU_ARP.1(2) | FAU_SAA.1 | YES |
| FDP_IFC.2 | FDP_IFF.1 | YES |
| FDP_IFF.1 | FDP_IFC.1 | YES |
| | FMT_MSA.3 | YES |
| FDP_IFF.6 | AVA.CCA.1 | YES |
| | FDP_IFC.1 | YES |
| FMT_MOF.1 | FMT_SMR.1 | YES |
| FMT_MSA.1 | FDP_IFC.1 | YES |
| | (FDP_ACC.1) | NO |
| | FMT.SMR.1 | YES |
| FMT_MSA.2 | ADV_SPM.1 | YES |
| | FDP_IFC.1 | YES |
| | FMT_MSA.1 | YES |
| | FMT_SMR.1 | YES |
| FMT_MSA.3 | FMT_MSA.1 | YES |
| | FMT_SMR.1 | YES |
| FPT_AMT.1 | None | |
| FPT_FLS.1 | ADV_SPM.1 | YES |
| FPT_PHP.1 | FMT_MOF.1 | YES |
| FPT_SEP.1 | None | |
| FPT_TRP.1 | None | |
| <u>Security requirements for the IT environment</u> | | |
| FAU_ARP.1.Env | FAU_SAA.1 | YES |
| FAU_GEN.1 | FPT_STM.1 | YES |
| FAU_SAA.1 | FAU_GEN.1 | YES |
| FAU_SAR.1 | FAU_GEN.1 | YES |
| FAU_STG.1 | FAU_GEN.1 | YES |
| FIA_UAU.1 | FIA_UID.1 | YES |
| FIA_UID.1 | None | |
| FMT_SMR.1 | FIA.UID.1 | YES |
| THA-REQ.1.Env | None | |
| FPT_STM.1 | None | |

Table 9: Security Requirements dependencies

The dependency FMT_MSA.1 -> FDP_ACC.1 is not required as FMT_MSA.1 -> FDP_IFC.1 is included (only one of these must be included according to CC).

Note1: FDP_IFF.6, FMT_MSA.1 and FMT_MSA.2 have a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

Note2: FMT_MSA.2 and FPT_FLS.1 have a dependency to ADV_SPM.1, which is covered by ADV_SPM.3.

8.4 TOE summary specification rationale

Table 10 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 covert 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.Self.Test | FPT_AMT.1 | The TOE self-test function performs an underlying abstract machine testing. |
| 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.Domain.Separation | FPT_SEP.1 | The domain separation function separates the TOE domain into non-secure network and secure network. |
| 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 10: TOE Security Functions satisfy SFRs

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

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.

9. CHANGES

This document is based on 3aq 21900 xaaa sczza Ed. 8.

Changes for edition 6.2:

- ST Document number changed to 24863
- Chapter 1.1 - TCB and firewall definition file identified
- Chapter 2.1 – Distinction of the two OTA modes added as explanation to the figure
- Chapter 2.2 – Updated with definition of TOE perimeter
- Chapter 2.4 and 2.5 updated to reflect new TOE definition
- Chapter 2.8 – figure updated to include loudspeaker
- Chapter 3.1 – assumptions A.SELF.TEST and A.OTA.ALARM added
- Chapter 4.3 – OE.SELF.TEST added
- Chapter 5.1.1 – updated
- Chapter 5.2.1 – FAU_ARP.1.Env added
- Chapter 5.2.4 added
- Chapter 6.1.1 updated
- Chapter 8 – Rationale - tables and text updated following the changes to the assumptions and security functional requirements stated above.

End of changes for edition 6.2.

Changes for edition 1p6.3 (included in edition 6.2.1)

- Chapter 1.1 – TOE identification is rewritten, 3aq 21564 ABAA variant is removed, and the specific version of the trusted kernel is stated.
- Chapter 4.1 – O.ALARM.FAILURE and O.ALARM.FW is updated with respect to what is performed by the TOE and OTA application regarding alarms.
- Chapter 6.2 – added that EAL5 is augmented with ALC_FLR.3
- Chapter 6.1.1, 8.3.1.1, and 8.3.1.2 is updated with respect to what is performed by the TOE and OTA application regarding alarms.
- 8.4 – SF.Security.Alarm – removed “if possible”
- Chapter 3.1, 4.3, 5.2.4, 8.3.2, 8.3.3 are changed because all periodic tests are run by the TOE, except the firewall test, which is initiated from the secure OTA application, but under surveillance by the TOE. A non-standard requirement denoted THA_REQ.1.Env has replaced FPT_AMT.1.Env in order to express this correctly.

End of changes for edition 1p6.3.

Changes for edition 6.2.1

- Chapter 1.1 – TOE module “OTA firewall definition file” is identified with variant and version.
- Chapter 1.1 – TOE module “OTA trusted kernel” is identified with specific version.
- Chapter 1.4 – Document identification in ref. [1] and [5] are corrected (new number and variant).
- Chapter 5.2 – table 3 updated: FPT_AMT.1.Env changed to THA_REQ.1.Env.

End of changes for edition 6.2.1.

Changes for edition 6.2.2

- Chapter 1.1 – version of the “OTA firewall definition file” is incremented due to the correction of FLIS 23899.

End of changes for edition 6.2.2.

Changes for edition 6.2.3

Change no. C5193

- Chapter 1.1 – new variant (HAAA) of the “OTA firewall definition file” added.

FLIS no. 24285, 24286 and 24290

- Trusted Kernel version updated from 6.2.1 to 6.2.2 due to Flaw Remediation.

End of changes for edition 6.2.3.

Changes for edition 6.2.4

Change no. C5220

- Chapter 1.1 – new variant and version of the “OTA firewall definition file” added.

End of changes for edition 6.2.4.