Huawei GBTS Version 100 Release 13 Security Target

Version: 1.16

Last Update: 2011-07-04

Author: Huawei Technologies Co., Ltd.

Index

Changes control

Version	Date	**Author**	Changes to previous version
V 1.13	2011-04-28	**ZhangLing**	---
V 1.14	2011-05-24	**ZhangLing**	Modifications to include M2000 access into the access control policy.
V 1.15	2011-06-05	**ZhangLing**	Modifications to as the observation from Epoche engineer.
V 1.16	2011-07-04	**ZhangLing**	Modifications to as the observation from Epoche engineer.

1 Introduction

This Security Target is for the evaluation of Huawei GBTS version 100 Release 13.

1.1 Security Target Reference

Title: Huawei GBTS Security target

Version: 1.16

Author: Zhang Ling

Publication date: 2011-7-4

1.2 Target of Evaluation (TOE) Reference

TOE name: Huawei GBTS

TOE version: Version 100 Release 13

TOE Developer: Huawei

TOE release date: 2011 -04-28

1.3 Target of Evaluation (TOE) Overview

The Huawei's GBTS can be widely used to support the wireless access of home and enterprise users. The Huawei's GBTS networking supports various access modes, including the FE, GE, optical fibber, microwave access, and satellite.

The GBTS product includes a BSC6900 unit which is an important Network Element (NE) of Huawei SingleRAN solution. It adopts the industry-leading multiple Radio Access Technologies (RATs), IP transmission mode, and modular design. In addition, it is integrated with the functions of the Radio Network Controller (RNC) and Base Station Controller (BSC), thus efficiently maintaining the trend of multi-RAT convergence in the mobile network.

The BSC6900 can be flexibly configured as a BSC6900 GSM, BSC6900 UMTS, or BSC6900 GU (GSM & UMTS) as required in different networks. The BSC6900 in independent mode refers to the BSC6900 GSM or the BSC6900 UMTS whereas the BSC6900 in integrated mode refers the BSC6900 GU.

The BSC6900 operates as an integrated NE to access the GSM&UMTS network and integrates the functions of the GSM BSC and the UMTS RNC. When the BSC6900 accesses the GSM network, the 3GPP R8 applies; when the BSC6900 accesses the UMTS network, the 3GPP R9 applies.

This ST contains a description of the security objectives and the requirements, as well as the necessary functional and assurance measures provided by the TOE. The ST provides the basis for the evaluation of the TOE according to the Common Criteria for Information Technology Security Evaluations (CC)

1.3.1 TOE usage

The GBTS possesses the following features:

1.High integration, reducing the overall size;
2.On an all-IP platform, thus supporting smooth upgrade;
3.Industry-leading technologies, delivering excellent performance;
4.Flexible networking.

The major security features implemented by GBTS and subject to evaluation are:

1. authentication

Operators using the GUI client to access the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.

If certificates are provided and deployed in network element and GBTS, the SSL/TLS connection between NE and M2000 can be selected through M2000 client. This connection implies the utilization of a special user registered in the GBTS.

2. Role_based access control

GBTS and BSC6900 implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations.

3. Fault Tolerance

There is a backup board for OMU unit and another board for the interface unit inside the BSC6900 unit of the TOE. The inter-board module works in active-standby mode, and switchover if failure in the active mode. Single point of failure is mitigated as the high availability feature applied.

4. Auditing

Audit records are created for security-relevant events related to the use of GBTS and BSC6900.

5. Communications security

GBTS and BSC6900 offers SSL/TLS channels for FTP, MML (man-machine language, which is kind of CLI), and BIN (Huawei’s private binary message protocol) access to the TOE and inter communication.

VLAN (Virtual Local Area Network) are implemented to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead.

ACL (Access Control List) implements Packet filtering features to restrict resource use via IP address, ports, etc. Those features protect the GBTS against various unauthorized access from unauthorized NEs.

6. Management of security functionality

The TOE offers management functionality for its security functionality.

7. Digital signature.

In the production and distribution phases, the digital signature scheme, protect the software package by message digest and signature.

1.3.2 TOE type

GBTS (GSM Base Transceiver Station) Software: The TOE implements basic functions of GBTS: security features, including system access control; auditing of security-relevant user activities; as well as the enforcement of network transmission against data peeking; system management to manage the security function of the GBTS.

1.3.3 Non TOE Hardware and Software

The TOE is GBTS and BSC6900 software packages. It is deployed on the boards GTMU for the GBTS, and in the operation & maintenance unit (OMU) and interface unit (PIU/AIU) for BSC6900. These hardware boards are TOE environment.

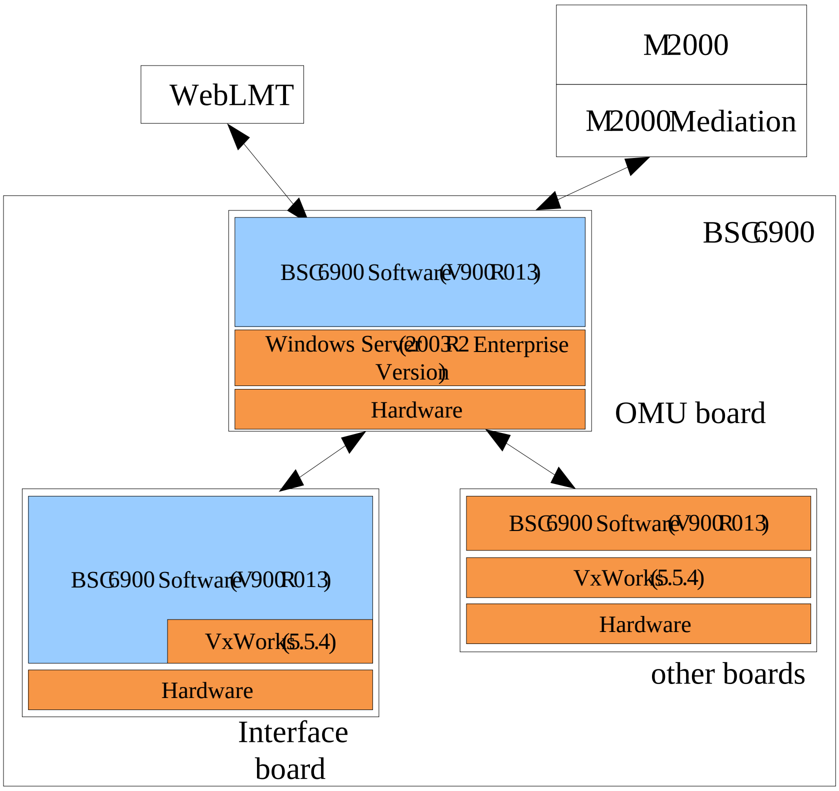


Figure1: Non TOE Hardware and Software environment for the MBSC

Application notes: In the above diagram, the light blue box area belongs in TOE while the orange box area belongs in TOE environment.

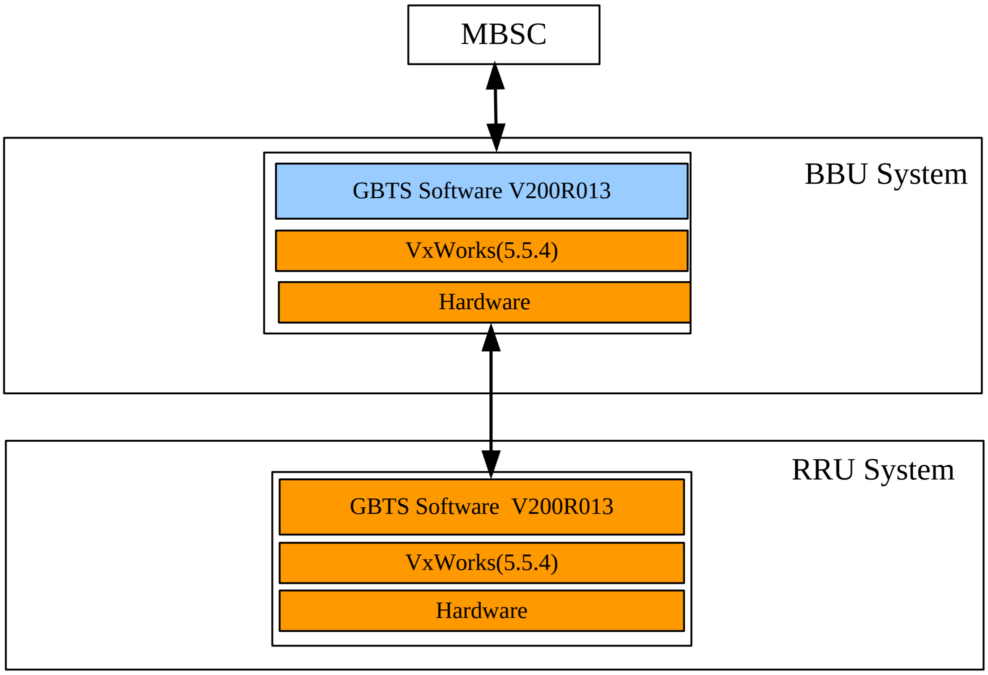


Figure1: Non TOE Hardware and Software environment for the GBTS

The interface between GBTS and MBSC is the Abis interface (3GPP protocol defined);

The interface between MBSC and core network is the A interface(3GPP protocol defined). RRU system connect to the BBU system in GTMU card by CPRI.

M2000 Mediation:

The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed.

The environment for TOE comprises the following components:

- the Windows operating system Windows Server 2003R2 Enterprise Version
- utilities, such as OfficeScan Anti-virus Software OfficeScan8.0 Version
- BSC6900 Physical Architecture
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through interfaces on GTMU within the TOE via a secure channel SSL.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.

- Operating system Vxworks , version 5.5.4
- An M2000 server providing management functions to the TOE.and M2000 version can be V2R10 or V2R11
- MBSC and GBTS together to complete WCDMA wireless communication access. MBSC version can be RAN13.

Logically, the hardware environment in the BSC6900 unit consists of the following three subsystems:

Switching Subsystem

The switching subsystem performs switching of traffic data, signaling, and OM signals.

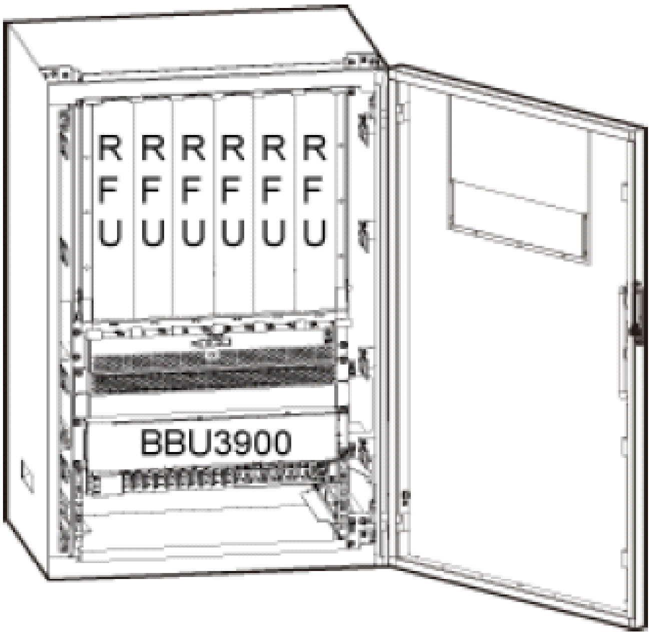
Service Processing Subsystem

The BSC6900 service processing subsystem performs the control functions defined in the 3GPP protocols and processes services of the BSC6900.

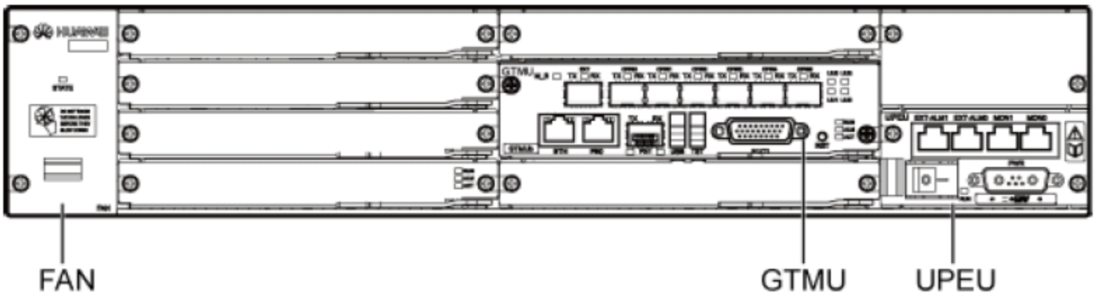
Clock Synchronization Subsystem

The clock synchronization subsystem provides clock signals for the BSC6900, generates the RNC Frame Number (RFN), and provides reference clock signals for base stations.

The following figure shows Huawei GBTS's physical structure:



The TOE belong to GBTS runs into the BBU3900 subrack, whose structure is as shown in the following figure:



The BBU3900 contains, at least, the following mandatory boards:

The GSM Timing and Main control unit (WMPT), which is the main board of BBU3900.

The Universal Power and Environment Interface Unit (UPEU), whose purpose is providing power to the whole BBU3900 subrack.

The FAN unit of the BBU3900 controls the fan speed, monitors the temperature of the FAN unit, and dissipates the heat from the BBU.

There are several GBTS type, including DBS3900, BTS3900, BTS3900A and BTS3900L.

DBS3900: The DBS3900 fully addresses operators' concerns over site acquisition, facilitates network planning and optimization, and reduces network deployment time. Thus, the DBS3900 enables operators to efficiently deploy a high-performance GSM/UMTS/LTE network with a low Total Cost of Ownership (TCO) by minimizing investment in electricity, space, and manpower.

BTS3900: The Huawei BTS3900 is the most compact indoor macro base station in the industry. It features large capacity, small size, and easy expansion.

BTS3900A: The BTS3900A is used in outdoor scenarios. The APM30H (Ver.B) or TMC11H is stacked on top of the radio frequency cabinet (RFC). Together they provide the power supply, surge protection, and other protections for the BBU3900 and RFUs, and adopt a natural ventilation mode for heat dissipation.

BTS3900L: The BTS3900L cabinet houses the BBU3900 and RF modules. In addition, it provides functions such as power distribution and surge protection. A single BTS3900L can have a maximum of 12 RF modules and 2 BBU3900s. This improves the integration of indoor sites, saves installation space, and facilitates smooth evolution.

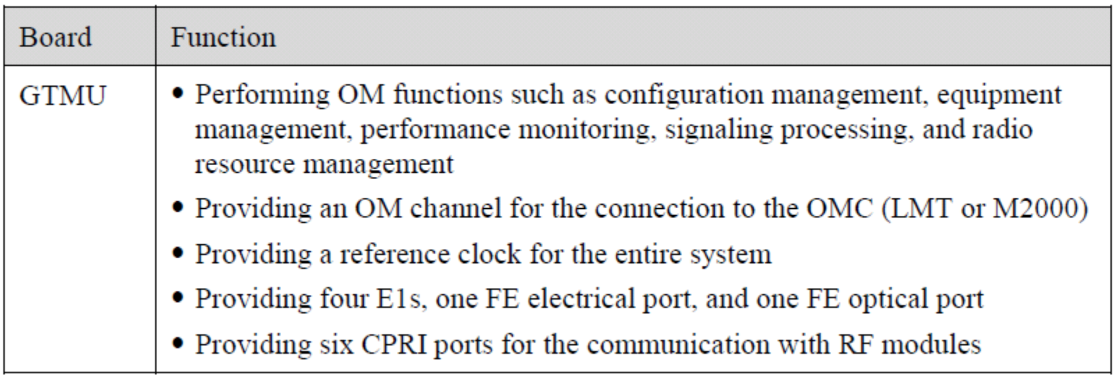
NodeB software is compatible with these types of stations above type, that is, in a different type of base station, the operation is the same set of software.

As a product family, the following table shows the physical boards of the TOE belong to MBSC:

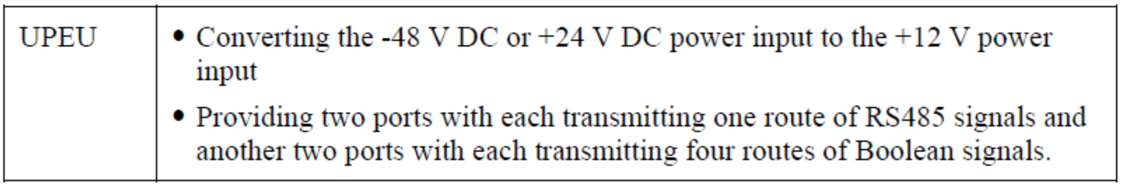
Board Type	Board Name	Function
OM board	OMUc	• Handles configuration management, performance management, fault management, security management, and loading management for the BSC6900. • Works as the OM agent for the LMT/M2000 to provide the BSC6900 OM interface for the LMT/M2000, thus achieving the communication between the BSC6900 and the LMT/M2000. • Works as the interface to provide the web-based online help. **Differences:** The OMUc board occupies only one slot and supports one hard disk.
Switching processing board	SCUb	• Provides MAC/GE switching and enables the convergence of ATM and IP networks. • Provides data switching channels. • Provides system-level or subrack-level configuration and maintenance. • Distributes clock signals for the BSC6900. **Differences:** The switching capability of the SCUb board is four times that of the SCUa board.
Clock processing board	GCGa	Obtains the system clock source, performs the functions of phase-lock and holdover, and provides clock signals. **Differences:** Unlike the GCUa board, the GCGa board can receive and process the GPS signals.
	GCUa	
Signaling processing board	SPUb	Manages user plane and signaling plane resources in the subrack and processes signaling.
Service processing board	DPUe	Processes CS services and PS services within the system.
Service identification board	NIUa	Provides the service identification function. It works with the service processing boards to schedule different types of services.
Interface processing board	AEUa	• Provides 32 channels of ATM over E1/T1. • Extracts clock signals and sends the signals to the GCUa or GCGa board.

Board Type	Board Name	Function
	AOUc	- Provides four channels over the channelized optical STM-1/OC-3 ports based on ATM protocols. - Supports ATM over E1/T1 over SDH or SONET. - Provides 252 E1s or 336 T1s. - Extracts clock signals and sends the signals to the GCUa or GCGa board.
	FG2c	- Provides 12 channels over FE electrical ports or 4 channels over GE electrical ports. - Supports IP over FE/GE.
	GOUc	- Provides four channels over GE optical ports. - Supports IP over GE.
	PEUa	- Provides 32 channels of IP over E1/T1. - Extracts clock signals and sends the signals to the GCUa or GCGa board.
	POUc	- Provides four channels over the channelized optical STM-1/OC-3 ports based on IP protocols, equivalent to 252 E1s or 336 T1s. - Supports IP over E1/T1 over SDH/SONET. - Extracts clock signals and sends the signals to the GCUa or GCGa board.
	UOIa	- Provides four channels over the unchannelized STM-1/OC-3c optical ports. - Supports ATM/IP over SDH/SONET. - Extracts clock signals and sends the signals to the GCUa or GCGa board.
	UOIc	- Provides eight channels over the unchannelized STM-1/OC-3c optical ports. - Supports ATM over SDH/SONET. - Extracts clock signals and sends the signals to the GCUa or GCGa board.

the following table shows the physical boards of the TOE belong to GBTS:



Board	Function
GTMU	• Performing OM functions such as configuration management, equipment management, performance monitoring, signaling processing, and radio resource management • Providing an OM channel for the connection to the OMC (LMT or M2000) • Providing a reference clock for the entire system • Providing four E1s, one FE electrical port, and one FE optical port • Providing six CPRI ports for the communication with RF modules



UPEU	• Converting the -48 V DC or +24 V DC power input to the +12 V power input • Providing two ports with each transmitting one route of RS485 signals and another two ports with each transmitting four routes of Boolean signals.

Table 2 shows interfaces available for the TOE belong to MBSC along with respective usage:

Boards	**Supported Interfaces and Usage**
OMUc	The following list shows a collection of interfaces which might be used during this evaluation for all models. • ETH interface, connector type RJ45, operation mode 10M/100M/1000M Base-TX auto-sensing, supporting half-duplex and full-duplex, compliant to IEEE 802.3-2002, used for connections initiated by users and/or administrators from a local maintenance terminal via HTTPS or SSH to perform management and maintenance operations. Management and maintenance through NMS workstation is not within the scope of this evaluation thus NMS related accounts should be disabled during the evaluation. • Console interface, connector type RJ45, operation mode Duplex Universal Asynchronous Receiver/Transmitter (UART) with electrical attribute RS-232, baud rate 9600 bit/s which can be changed as required, used for users and/or administrators to connect to console for the on-site configuration of the system.
FG2c	• The interfaces boards are used for incoming and outgoing network traffic, which support VLAN, IP_based ACL, anti-DDoS attack characteristics.

Table 2: Interfaces Specifications

This table shows interfaces available for the TOE belong to GBTS along with respective usage:

Boards	Supported Interfaces and Usage
GTMU	The following list shows a collection of interfaces which might be used during this evaluation for all models. • ETH interface, connector type RJ45, operation mode 10M/100M Base-TX auto-sensing, supporting half-duplex and full-duplex, compliant to IEEE 802.3-2002. • Console interface, connector type RJ45, operation mode Duplex Universal Asynchronous Receiver/Transmitter (UART) with electrical attribute RS-232, baud rate 9600 bit/s which can be changed as required, used for users and/or administrators to connect to console for the on-site configuration of the system.

1.4 TOE Description

The TOE is composed of the BSC6900 unit and the GBTS unit.

The main elements of the BSC6900 are:

OM Subsystem

The OM subsystem enables the management and maintenance of the BSC6900 in the following scenarios: routine maintenance, emergency maintenance, upgrade, and capacity expansion.

Interface Processing Subsystem

The interface processing subsystem provides transmission ports and resources, processes transport network messages, and enables interaction between the BSC6900 internal data and external data.

Transport subsystem:

The Transport subsystem can provide the function below:

transport configuration,traffic forwording and DHCP ,etc.

The main elements of of the GBTS are:

Transport subsystem:

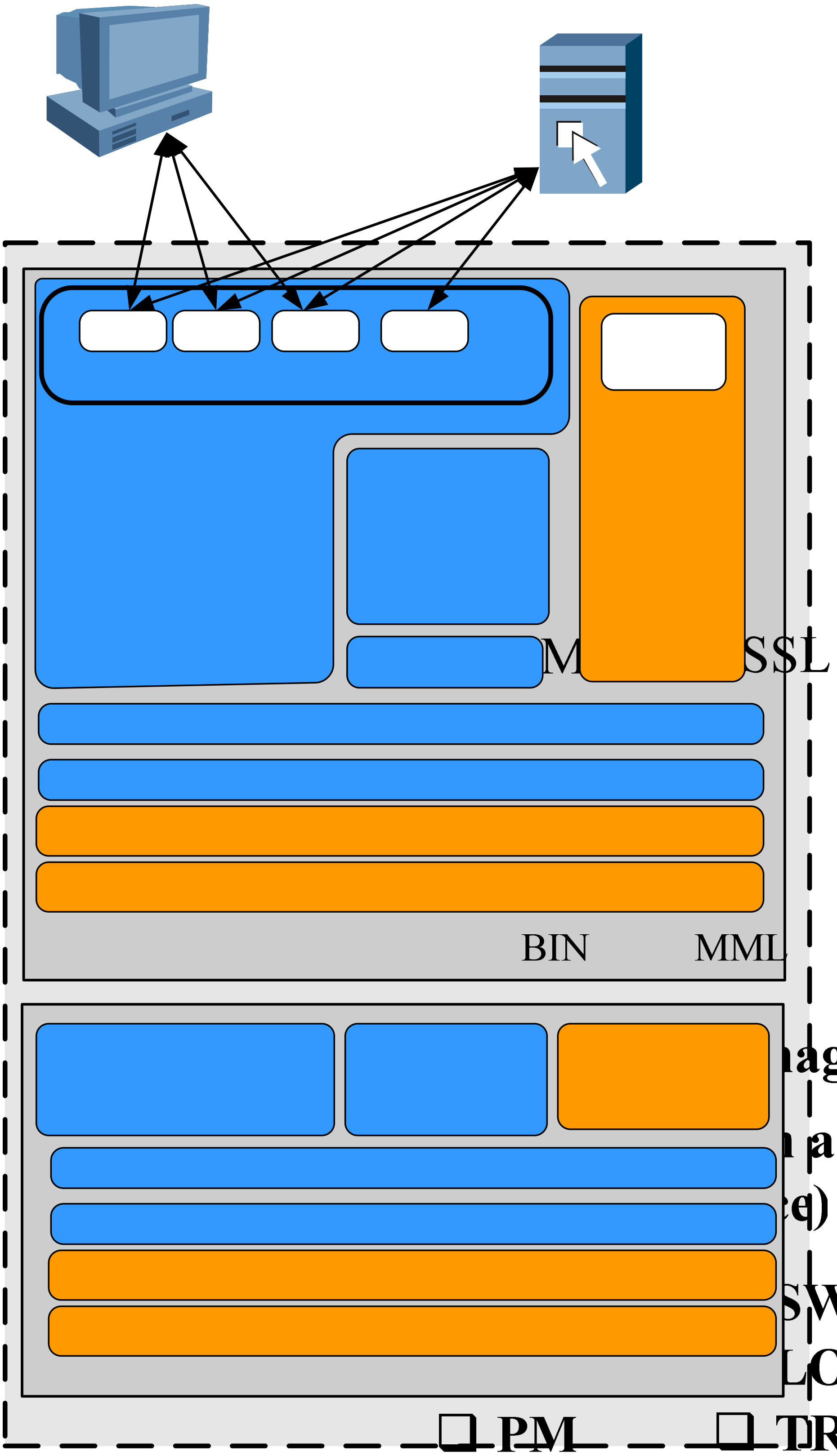
The Transport subsystem can provide the function below:

transport configuration,traffic forwording and DHCP,VLAN separation,etc.

1.4.1 Logical Scope

In the above diagram, Only Security-related function is shown.

But in the GBTS and MBSC, there are also the other functions.



agement flows)

and

e)

SWM

LOG

TM

Ma

❑ V

❑ T

❑ PM ❑ TRACE

❑ FM ❑ TM

❑ ADAPTER

Depra SSP(Runti

Figure 1 TOE Software architecture

As shown in Figure 1 Software Architecture, the TOE is entirely composed by software. The Operating System, and other software provided by particular products belong to the TOE environment. The TOE itself includes OM, Product Service, Transport Management, TRAN, CPBSP and Dopra SSP.

For each of the identified parts of the TOE, a correspondence between them and the TOE security functionality can be achieved. That way, for each part, the appropriate security associated functionality is indicated in the following table:

Element	Part	Associated security functionality
Security Function Interface	All the interfaces	Resource management
	Communications through the following protocols: BIN: Huawei's private binary message protocol. MML: Man-Machine Language. FTP: File transmission Protocol	Communications security
Operation and Maintenance (OM)	NMI: network management interface: which is the interface for external element	NA
	CFG: Configuration Management, responsible for the managed elements configuration.	Security functionality management
	PM: Performance management, responsible for the calculation of performance data and the storage of it.	NA
	FM: Fault management, which include fault and alarm monitoring.	NA
	SWM: Software management, responsible for software upgrade and rollback.	Digital signature
	LOG: Responsible for the audit and storage of security log and operational log.	Auditing
	TRACE: Responsible for the trace messages which show the state of the BS and MS within the GBTS network.	NA

	RRE: Common service, responsible for basic service for other modules	NA
Transport Management (TM)	VPP: Voice Protocol Platform, which is composed of voice and signal processing component, such as XML Parser, Stream Control Transmission Protocol (SCTP) and Signaling ATM Adaptation Layer (SAAL). VISP: Versatile IP and Security Platform, which provides TCP / IP protocol stack management interface. TLM: Transport layer management. The functions include control and supervision of the transport bearer (data forwarding) functions, maintaining the transport resource assignment to product services.	Communication Security
TRAN	Huawei's wireless transmission platform, which provide hardware driver management interface.	Communication Security
DOPRA SSP (Runtime Environment)	Provide Operating System mid-ware layer. It function includes: Operation System Adapter, Memory management, Timer management, etc.	NA
CPBSP	Provide a standard API interface for the hardware.	NA

The logical boundary is represented by the elements indicated in the GBTS and BSC elements within the dashed border. So, the TOE’s logical scope with supporting network devices of the environment is as follows.

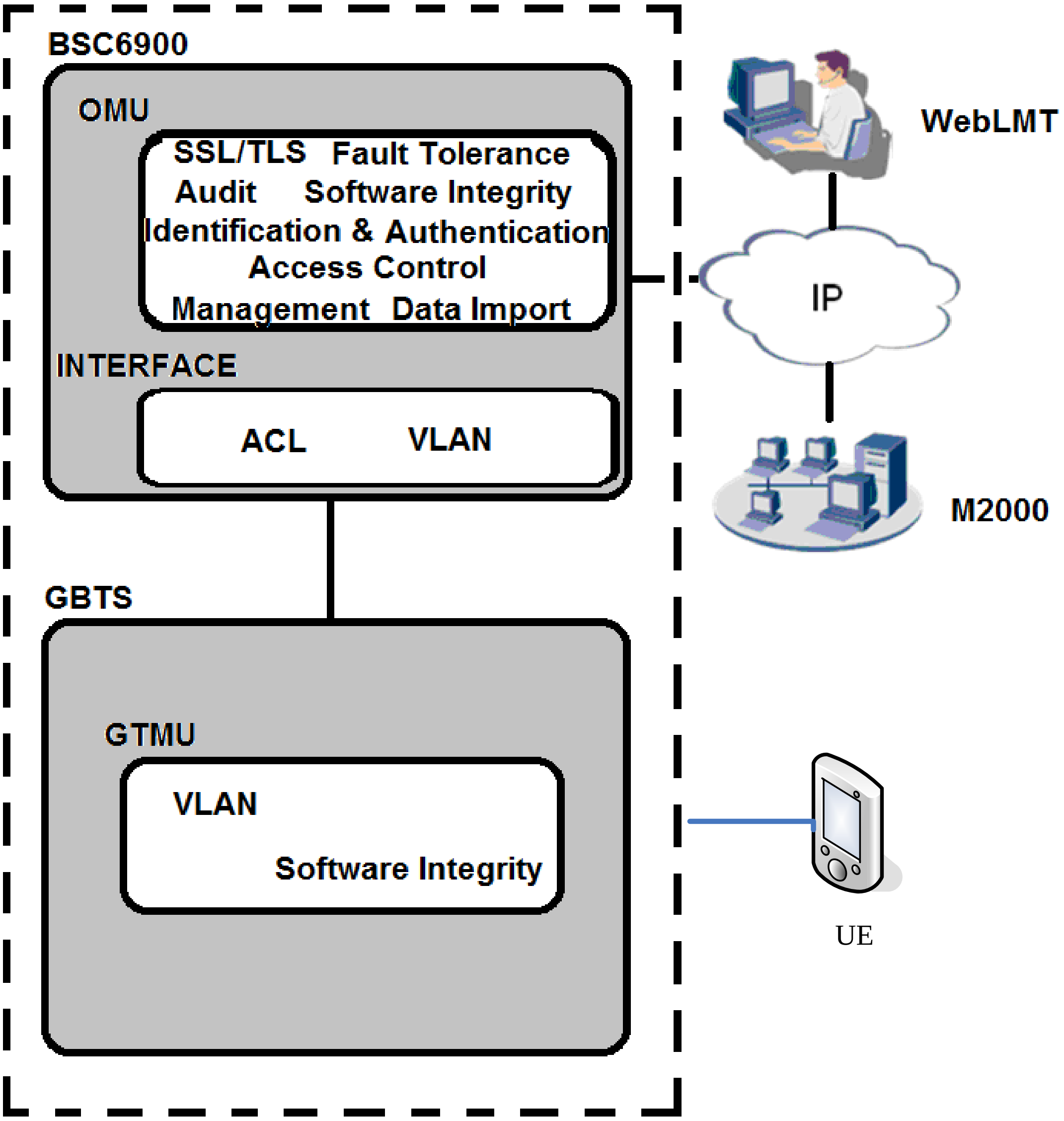


Figure 2 TOE logical scope

GBTS software includes two parts, one part is in GBTS hardware and the other part is in BSC hardware. Between BSC and GBTS is Abis interface,And the Abis interface bears User traffic, signaling and OAM data . These data packets are transmited with Huawei proprietary protocol.

The TOE controls the flow (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine.

System control and security managements are performed either through interfaces on OMU via a secure channel enforcing SSL/SSH/TLS.

The interface processing subsystem is in charge of controlling flow (datagrams) between network interfaces. The elements under the interface processing subsystem control are NodeB, GBTS, MSC and SGSN. This control is performed by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine. Also, a session establishment control is performed in order to accept or deny connections. In case of failure, the fault tolerance procedure will switch the active interface board with the stand-by interface board.

The OM subsystem is in charge of the system control and security managements of the BSC6900. This management is performed via a secure channel enforcing SSL/SSH/TLS. Also, it provides a controlling flow of the connection with the M2000 and WebLMT elements. The same fault tolerance procedure is implemented in the OMU, so in case of failure, the switch with the stand-by board will remains the system operative.

Based on logical scope described so far, a list of configuration is to be added:

- For management via the Ethernet interface, authentication is always enabled.
- Authentication of users via RSA when using SSH connections is supported.

1.4.2 Physical Scope

The release packages for GBTS are composed of software and documents for the BSC6900 and the GBTS units.

The BSC6900 software packages are in the form of compressed files.

The software and documents for the TOE belong to MBSC is the following:

Software and Documents	Description	Remark
BSC6900 V900R013 VER.rar	Product software package stored in the OMU board	
Interface.bin	Interface board software package contained in the OMU board and loaded in the interface board.	

Software and Documents	Description	Remark
(For Customer)BSC6900 GSM Product Documentation (V900R013)(HDX)-EN .zip (For Customer)BSC6900 UMTS Product Documentation (V900R013)(HDX)-EN .zip (For Customer)BSC6900 GU Product Documentation (V900R013)(HDX)-EN .zip	This CD-ROM integrates Huawei BSC6900 V900R013 product documentation. The product documentation covers the planning, installation, commissioning, and maintenance of the BSC6900 system.	The guidance documents of BSC 6900 UMTS are part of the TOE.

The release packages for GBTS are composed of software and documents. The GBTS software packages are in the form of binary compressed files.

The GBTS software packages can be downloaded and stored in the GTMU board, and then, they will be checked up, unpacked, and then distributed to each board module, such as GTMU, UPEU .

The software and documents for the TOE belong to GBTS is the following:

Software and Documents	Description	Remark
download.zip	Board software package (In the form of binary compressed files)	The software packages which are the TOE will be digitally signed to ensure their legitimacy and integrity.
vercfg.xml	Version description files	
download.sgn	Board software package signature files	These signature files are generated by Huawei digital signature tool
vercfg.sgn	Version description signature files	
GBTS documents include (For Customer)3900 Series GSM BTS Product Documentation (V100R013C00_01)(HDX) -EN 3900 GSM Series BTS V100R013C00 Release Notes 3900 GSM Series BTS V100R013C00 Upgrade Guide	Release notes, MML command reference, and alarm reference.	The guidance documents of GBTS are part of the TOE.

2 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The CC version of [CC] is 3.1R3.

The methodology to be used for evaluation is CEM3.1 R3.

This ST is EAL3 conformant as defined in [CC] Part 3 with the augmentation of ALC_CMC.4, ALC_CMS.4.

No conformance to a Protection Profile is claimed.

3 TOE Security problem definition

3.1 TOE Assets

The information assets to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, audit records, etc.) and other information that the TOE facilitates access to (such as system software, patches) are all considered part of information assets.

The TOE consists of the following assets:

Asset	Description	Asset value
A1.Software and patches	The integrity and confidentiality of the system software and the patches when in transit across the management network should be protected from modification and disclosure.	Integrity Confidentiality
A2.Stored configuration data	The integrity and confidentiality of the stored configuration data should be protected. Configuration data includes the security related parameters under the control of the TOE (such as user account information and passwords, audit records, etc).	Integrity Confidentiality
A3. In transit configuration data	The integrity and confidentiality of the configuration data when travelling in the management network.	Integrity Confidentiality
A4.Availability	Availability of the services provided by the TOE.	Availability

3.2 Threats

This section of the security problem definition shows the threats to be countered by the TOE, its operational environment, or a combination of both. The threat agents can be categorized as either:

The agents of the threat:

Agent	Description
Eavesdropper	An eavesdropper from the management network served by the TOE is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.
External attacker	An unauthorized agent from the outside of the system who tries to break-into the management system and change the configuration data of the TOE and decrease the system performance.
Restricted authorized user	An authorized user of the TOE in the management network who has been granted authority to access certain information and perform certain actions.

In the first and second cases, the users are assumed to be potentially hostile with a clear motivation to get access to the data. In the last case, all authorized users of the TOE are entrusted with performing certain administrative or management activities with regard to the managed device. Consequently, organizational means are expected to be in place to establish a certain amount of trust into these users. However, accidental or casual attempts to perform actions or access data outside of their authorization are expected. The assumed security threats are listed below.

3.2.1 Threats by Eavesdropper

Threat: T1. InTransitConfiguration	
Attack	An eavesdropper in the management network succeeds in accessing the content of the MBSC file while transferring, violating its confidentiality or integrity.
Asset	A3. In transit configuration data
Agent	Eavesdropper

Threat: T2. InTransitSoftware	
Attack	An eavesdropper in the management network succeeds in accessing the content of the MBSC software/patches while transferring, violating its confidentiality or integrity.
Asset	A1.Software and patches
Agent	Eavesdropper

3.2.2 Threats by Internal Attacker

Threat: T3.UnwantedNetworkTraffic	
Attack	Unwanted network traffic sent to the TOE will cause the TOE's processing capacity for incoming network traffic to be consumed thus failing to process legitimate traffic. This may further causes the TOE fails to respond to system control and security management operations.
Asset	A4.Availability
Agent	External Attacker

Threat: T4.UnauthenticatedAccess	
Attack	An attacker in the management network gains access to the TOE disclosing or modifying the configuration date stored in the TOE in a way that is not detected.
Asset	A2.Stored configuration data
Agent	External Attacker

3.2.3 Threats by restricted authorized user

Threat: T5.UnauthorizedAccess	
Attack	A user of the TOE authorized to perform certain actions and access

	certain information gains access to commands or information he is not authorized for.
Asset	A2.Stored configuration data
Agent	Restricted authorized user

3.3 Assumptions

3.3.1 Physical

- **A.PhysicalProtection**

It is assumed that the TOE is protected against unauthorized physical access.

3.3.2 Personnel

- **A.TrustworthyUsers**

It is assumed that the organization responsible for the TOE and its operational environment has measures in place to establish trust into and train users of the TOE commensurate with the extent of authorization that these users are given on the TOE. (For example, super users and users that are assigned similar privileges are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them.)

3.3.3 Connectivity

- **A.NetworkSegregation**

It is assumed that the network interfaces that allow access to the TOE’s user interfaces are in a management network that is separated from the public networks.

3.3.4 Support

- **A.Support**

The operational environment must provide the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

3.3.5 OperationSystem

- **A.OperationSystem**

It is assumed that the operation system of the TOE' environment is secure.

3.3.6 Utilities

- **A.Utilities**

It is assumed that the utilities of the TOE' environment are secure.

3.3.7 Authentication

- **A. Identification and Authentication**

It is assumed that the GBTS's identification and authentication is accomplished by the MBSC unit of the TOE. Each user need to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

3.4 Organizational Policies

3.4.1 P.Audit

The TSF shall be able to generate an audit record of the auditable events, which associate with the identity of the user that caused the event. The TSF shall protect the stored audit records in the audit trail from unauthorized deletion. The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

3.4.2 P.RoleManagement

Different people access the FSF needs to be divided according to different roles with different permissions, as far as possible the user has the minimum required permissions.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Forwarding** The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds with a configured route for the destination address of the packet.
- **O.SecureCommunication** The TOE shall provide a secure remote communication channel for remote administration of the TOE via SSL.
- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- **O.Authentication** The TOE must authenticate users of its user access.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.SoftwareIntegrity** The TOE must provide functionality to verify the integrity of the received software patches.
- **O.RoleManagement** The TOE shall provide role management functionality: different people access the FSF is divided according to different roles with different permissions, as far as possible the user has the minimum required permissions.
- **O.FaultTolerance** The TOE shall provide the functionality of fault tolerance to remain the system operative against any failure or denial of service attack.

4.2 Objectives for the Operational Environment

- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide protection to the network in which the TOE hosts by separating it from the application (or public) network.
- **OE.OperationSystem** The operation system of the TOE' environment is secure.

- **OE.Utilities** The TOE need some utilities to finish some special function such as OfficeScan to anti-virus attack.
- **OE.Support** Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.
- **OE. TrustworthyUsers** Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective is at least covered by one threat or policy.

	T1.InTransitConfiguration	T2.InTransitSoftware	T3.UnwantedNetworkTraffic	T4.UnauthenticatedAccess	T5.UnauthorizedAccess	A.PhysicalProtection	A.TrustworthyUsers	A.NetworkSegregation	A.Support	A.OperationSystem	A.Utilities	P.Audit	P.RoleManagement	A.Identification & Authentication
O.Authentication				X	X									X
O.Authorization					X									
O.SecureCommunication	X	X	X	X	X									
O.SoftwareIntegrity		X												
O.Forwarding			X											
O.Audit												X		
O.RoleManagement													X	
O.FaultTolerance			X											

OE. Physical				X	X	X								
OE.NetworkSegregation								X						
OE.OperationSystem										X				
OE. Utilities											X			
OE. Support									X					
OE. TrustworthyUsers					X		X							

Table 4: Mapping Objectives to Threats

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T1.InTransitConfiguration	The threat T1.InTransitConfiguration is countered by requiring communications security via SSL for network communication between entities in the management network and the TOE (O.SecureCommunication).
T2. InTransitSoftware	The threat T2.InTransitSoftware is countered by O.SecureCommunication which establishes a secure communication channel between the TOE and external entities in the management network. This threat is also countered by O.SoftwareIntegrity: when a software package is loaded, its message digest and signature are verified.
T3.UnwantedNetworkTraffic	The threat T3.UnwantedNetworkTraffic is directly counteracted by the security objective for the TOE O.Forwarding. The security objective O.SecureCommunication counteracts the threat by preventing the reception of unwanted network traffic from non-secure connections. The security objective O.FaultTolerance protects the system availability and performance against

	possible denial of service attacks by the unwanted network traffic.
T4.UnauthenticatedAccess	The threat T4.UnauthenticatedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism for the users in the management network. The security objective for the operational environment OE.Physical contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified. The security objective O.SecureCommunication counteracts the threat by preventing the reception of authentication requests from non-secure connections.
T5.UnauthorizedAccess	The threat T5.UnauthorizedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism for the users in the management network. It is also countered by requiring the TOE to implement an access control mechanism (O.Authorization). It is also countered by requiring the TOE to implement a trusted path between TOE and its users (O.SecureCommunication) so the user credentials cannot be captured. The security objective for the operational environment OE.TrustworthyUsers contributes to the mitigation of this threat requiring the users to be responsible with their passwords. The security objective for the operational environment OE.Physical contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified

Table 6: Sufficiency analysis for threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.Physical	This assumption is directly implemented by the security objective for the environment OE.Physical.
A. TrustworthyUsers	This assumption is directly implemented by the security objective for the environment OE. TrustworthyUsers.
A.NetworkSegregation	This assumption is directly implemented by the security objective for the environment OE.NetworkSegregation.
A.Support	This assumption is directly implemented by the security objective for the environment OE.Support
A.OperationSystem	This assumption is directly implemented by the security objective for the environment OE.OperationSystem
A.Utilities	This assumption is directly implemented by the security objective for the environment OE.Utilities.

Table 7: Sufficiency analysis for assumptions

The following rationale provides justification that the security objectives are suitable to counter each individual policy and that each security objective tracing back to a policy:

Policy	Rationale for security objectives
P.Audit	This policy is directly implemented by the security objective for the TOE O.Audit
P.RoleManagement	This policy is directly implemented by the security objective for the TOE O.RoleManagement

Table 8: Sufficiency analysis for policies

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF 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 [***selection:*** ***not specified***] level of audit; and

c) [***assignment:*** ***The following auditable events:***

i. user activity

1. login, logout

2. operation requests

ii. user management

1. add, delete, modify

2. password change

3. authorization modification

4. locking, unlocking (manual or automatic)

iii. user group management

1. add, delete, modify

iv. command group management

1. add, delete, modify

v. Fault tolerance

1. Stand-by board switch to active board]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), 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, [***assignment:*** ***workstation IP (if applicable), user (if applicable), and command name (if applicable).***]

FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [***assignment***: ***users authorized per FDP_ACF.1/Local users, FDP_ACF.1/Doamin users and FDP_ACF.1/EMSCOMM user***] with the capability to read [***assignment***: ***all information***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: selection] of audit data based on [***assignment: source operator domain name IP address start time end time log type log level.***]

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion

FAU_STG.1.2 The TSF shall be able to [***selection***: ***prevent***] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [***assignment***: ***delete the oldest files***] if the audit trail exceeds [***assignment***: ***an administrator configured value***].

6.1.2 Cryptographic Support (FCS)

FCS_COP.1/Digital Signature Cryptographic operation

FCS_COP.1.1 The TSF shall perform [***assignment: digital signature verification***] in accordance with a specified cryptographic algorithm [***assignment: RSA with underlying SHA-256***] and cryptographic key sizes [***assignment: 1024bits***] that meet the following: [***assignment: none***]

FCS_COP.1/Channel encryption Cryptographic operation

FCS_COP.1.1 The TSF shall perform [***assignment: cipher and decipher of TOE access channels***] in accordance with a specified cryptographic algorithm [***assignment: algorithms supported by SSL***] and cryptographic key sizes [***assignment: key sizes supported by SSL***] that meet the following: [***assignment: none***].

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***assignment***: ***cryptographic key generation supported by SSL***] and specified cryptographic key sizes [***assignment***: ***key sizes supported by SSL***] that meet the following: [***assignment***: ***none***].

6.1.3 User Data Protection (FDP)

FDP_ACC.2/Local users Complete access control

FDP_ACC.2.1 The TSF shall enforce the [***assignment: GBTS local users access control policy***] on [***assignment: Local users as subjects and Commands as objects***] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/Local users Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***assignment: GBTS local users access control policy***] to objects based on the following: [***assignment:***

Subjects

Local Users, security attributes:

i. User name

ii. Operational rights

Objects

Commands, security attributes:

i. Command name

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment***: ***the local user has execution permission of the command targeted by the request depending on the operational rights of the local user***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment: None*** **].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment: None***]

FDP_ACC.2/Domain users Complete access control

FDP_ACC.2.1 The TSF shall enforce the [***assignment: GBTS domain users access control policy***] on [***assignment: Domain users as subjects and Commands as objects***] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/Domain users Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***assignment: GBTS domain users access control policy***] to objects based on the following: [***assignment:***

Subjects

Domain Users, security attributes:

i. User name

ii. Operational rights

Objects

Commands, security attributes:

i. Command name

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment***: ***the domain user has execution permission of the command targeted by the request depending on the operational rights of the domain user***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment: None*** **].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment: None***]

FDP_ACC.2/EMSCOMM user Complete access control

FDP_ACC.2.1 The TSF shall enforce the [***assignment: GBTS EMSCOMM user access control policy***] on [***assignment: EMSCOMM user as subject and Commands as objects***] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/EMSCOMM user Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***assignment: GBTS EMSCOMM user access control policy***] to objects based on the following: ***[assignment:***

Subject

EMSCOMM, security attributes:

i. User name

ii. Operational rights

Objects

Commands, security attributes:

i. Command name

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment: the EMSCOMM user has execution permission of the command targeted by the request depending on the operational rights of the domain user***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment: None*].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment: None***]

FDP_ITC.1 Import from outside TSF control

FDP_ITC.1.1 The TSF shall enforce the [***assignment: GBTS local user, domain user and EMSCOMM user access control policy***] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [***assignment: none***].

6.1.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***selection: an administrator configurable positive integer within [assignment: 1 and 5]]*** unsuccessful authentication attempts occur related to [***assignment: authentication through the WebLMT by local users. The counter for these attempts is reset each time the user remains in the session a time frame configurable by administrator either between 1 and 60 minutes.***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***selection: surpassed***], the TSF shall [***assignment: lockout the account for an administrator configurable duration either between 1 and 65535 minutes***].

Application note: The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the BSC6900 by automatic method and not by user and password.

Domain users are authenticated in the M2000 element of the TOE environment, so they are not considered in this requirement neither by the TOE authentication functionality.

FIA_ATD.1/Local users User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment:***

*a) **Username***

*b) **User groups***

*c) **Password***

*d) **Number of unsuccessful authentication attempts since last successful authentication attempt***

*e) **Login allowed start time***

*f) **Login allowed end time***

*g) **Password expiration date***

*h) **Account expiration date***

*i) **Lock status***

*j) **Operational rights***

]

FIA_ATD.1/Domain users User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment:***

*a) **Username***

*b) **Password***

*c) **Operational rights***

]

FIA_ATD.1/ EMSCOMM user User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment:***

*a) **Username***

*b) **Operational rights***

]

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet:

[***assignment:***

a) ***an administrator configurable minimum length between 6 and 32 characters, and***

b) ***an administrator configurable combination of the following:***

i. at least one lower-case alphanumerical character,

ii. at least one upper-case alphanumerical character,

iii. at least one numerical character,

iv. at least one special character.]

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [***assignment***:

a) Authentication for Local Users

b) Authentication for Domain Users

c) Authentication for EMSCOMM user

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***assignment***:

a) Local Users are authenticated in BSC6900 by user and password stored in BSC6900

b) Domain users authentication is delegated in the M2000 management element of the environment by user and password

c) EMSCOMM user is authenticated in BSC6900 by a special arithmetic procedure common to both parties, BSC6900 and M2000.

].

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Security Management (FMT)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [***assignment:*** ***GBTS local user, domain user and EMSCOMM user access control policy***] to restrict the ability to [***selection:*** ***query and modify***] the security attributes [***assignment:*** ***password, user group, login allowed start time and end time of local users***] to [***assignment****: users with the appropriate operational rights*].

Application Note: The ability to query and modify the local users' information is provided to the users by assigning certain operational rights. The roles or user groups maintained in the system are just a mechanism to assign operational rights to the users. Then, the assignment of the requirement refers the "users with the appropriate rights". This is detailed in the TOE summary specification.

Application note: The security attributes of the EMSCOMM user are accessible for query neither modify to any user of the system. This is detailed in the TOE specification summary.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [***assignment:*** ***GBTS local user, domain user and EMSCOMM user access control policy***] to provide [***selection:*** ***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***assignment:*** ***administrator defined roles with the appropriate rights***] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***assignment:***

a) ***local user management***

b) ***user groups management***

c) ***commands groups management***

d) ***local users authorization management***

e) ***modification of the password policy***

f) ***Audit size limit***

g) ***enabling/disabling SSL/TLS***

h) ***VLAN configuration***

i) ***IP-based access control configuration***

]

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [***assignment:***

a) ***Guest***

b) ***User***

c) ***Operator***

d) ***Administrator***

e) ***Custom***]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note: These roles are only applicable to the local users. The domain users are not maintained in the BSC6900, no role neither user group is assigned to a domain user. Also, the EMSCOMM user can not be assigned to any role. This is detailed in the TOE specification summary.

6.1.6 TOE access (FTA)

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [***assignment: time interval of user inactivity which can be configured***].

FTA_TSE.1/SEP TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [***assignment:***

a) ***Protocol type***

b) ***Source IP address***

c) ***Source port***

d) ***Destination IP address***

e) ***Destination port***

f) ***VLAN id***]

Application note: This requirement addresses the VLAN separation and IP based ACLs to avoid resource overhead.

FTA_TSE.1/MGT TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [***assignment:***

a) ***Login allowed start time***

b) ***Login allowed end time***

c) ***Password expiration date***

d) ***Account expiration date***

e) ***Lock status***]

6.1.7 Fault tolerance

FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur :[***assignment: process failure, network card failure, OMU failure***].

6.1.8 Trusted Path/Channels (FTP)

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***selection: remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***selection: disclosure***].

FTP_TRP.1.2 The TSF shall permit [***selection: remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***selection: TOE usage***]

Application note: This requirement addresses the secure channel established with SSL/TLS in the management network.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

	O.Audit	O.Authentication	O.Authorization	O.SecureCommunication	O.Forwarding	O.SoftwareIntegrity	O.RoleManagement	O.FaultTolerance
FAU_GEN.1	×							
FAU_GEN.2	×							
FAU_SAR.1	×							
FAU_SAR.3	×							
FAU_STG.1	×							
FAU_STG.3	×							
FCS_COP.1/Digital Signature						×		
FCS_COP.1/Channel Encryption				×				
FCS_CKM.1				×				
FDP_ACC.2/Local users			×				×	
FDP_ACC.2/Domain users			×				×	
FDP_ACC.2/EMSCOMM user			×				×	
FDP_ACF.1/Local users			×				×	
FDP_ACF.1/Domain users			×				×	
FDP_ACF.1/EMSCOMM user			×				×	
FDP_ITC.1								×
FIA_AFL.1		×						

FIA_ATD.1/Local users		×	×					
FIA_ATD.1/Domain users		×	×					
FIA_ATD.1/EMSCOMM user		×	×					
FIA_SOS.1		×						
FIA_UAU.2		×						
FIA_UAU.5		×						
FIA_UID.2	×	×	×					
FMT_MSA.1			×				×	
FMT_MSA.3			×					
FMT_SMF.1		×	×	×			×	
FMT_SMR.1			×				×	
FTA_SSL.3		×	×					
FTA_TSE.1/SEP					×			
FTA_TSE.1/MGT		×	×					
FRU_FLT.2								×
FTP_TRP.1				×				

Table 8: Mapping SFRs to objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the authentication mechanism (FIA_UID.2). Audit records are in a string format.

	Selection based on parameters values is provisioned to read and search these records (FAU_SAR.1, FAU_SAR.3). The protection of the stored audit records is implemented in FAU_STG.1. Functionality to delete the oldest audit file is provided if the size of the log files becomes larger than the size specified by the administrators (FAU_STG.3).
O.SecureCommunication	All the channels accessing the TOE are implemented over SSL, so these channels are encrypted and protected against the disclosure of the information transmitted (FCS_COP.1/Channel Encryption, FTP_TRP.1). The keys used for the channels encryption are generated as part of the SSL connection establishment process (FCS_CKM.1).
O.Forwarding	Before other NEs send packet to MBSC, it is needed to create channels. It will check IP source address, IP destination address, protocol type, source port and destination port. If the matching is fail, the packet will not forward. (FTA_TSE.1/SEP)
O.SoftwareIntegrity	The software integrity objective is directly implemented with FCS_COP.1/Digital Signature, so the TOE performs digital signature verification over the software.
O.Rolemanagement	The requirements for access control on the management network are modeled in FDP_ACC.2/Local users, FDP_ACC.2/Domain users, FDP_ACC.2/EMSCOMM user, FDP_ACF.1/Local users, FDP_ACF.1/Domain users, FDP_ACF.1/EMSCOMM user. The operational rights are assigned in relation to the different

	roles defined in the system (FMT_SMR.1). Management functionality for access control is provided in FMT_SMF.1 and FMT_MSA.1.
O.Authentication	User authentication is implemented by FIA_UAU.5. Also, each user must be identified and authenticated before operating with the TOE supported by FIA_UID.2 and FIA_UAU.2. The necessary user attributes (passwords) are spelled out in FIA_ATD.1/Local users, FIA_ATD.1/Domain users and FIA_ATD.1/EMSCOMM user. The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for logon (FTA_TSE.1/MGT), and a password policy (FIA_SOS.1). Management functionality is provided in FMT_SMF.1. Also the authentication mechanism supports FTA_SSL.3.
O.Authorization	Access control is based on the definition of users as subject and commands as objects. The requirement for access control is spelled out in FDP_ACC.2/Local users, FDP_ACC.2/Domain users and FDP_ACC.2/EMSCOMM user. The access control policies are modeled in FDP_ACF.1/Local users, FDP_ACF.1/Domain users, FDP_ACF.1/EMSCOMM user. Unique user IDs are necessary for access control provisioning (FIA_UID.2), and user-related attributes are spelled out in FIA_ATD.1/Local users, FIA_ATD.1/Domain users and FIA_ATD.1/EMSCOMM user. The user roles,

	providing the corresponding operational rights are defined in FMT_SMR.1. The termination of an interactive session is provided in FTA_SSL.3. Management functionality for the definition of access control policies is provided in FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1.
O.FaultTolerance	The fault tolerance is covered by the security requirement FRU_FLT.2. Backup boards in stand-by mode take the active state to replace the faulty boards. The information from the active boards is firstly exported to external devices and then imported to the new active boards (FDP_ITC.1).

Table 9: SFR sufficiency analysis

6.2.3 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution

FAU_GEN.1	FPT_STM.1	Not satisfied. The time is obtained from the environment, either from the hardware or from an external NTP server.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/Digital Signature	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	The key for the digital signature verification is included inside the software package sent to the user. The TOE does not delete keys, they are stored in the package in order to re-install the product when necessary.
FCS_COP.1/Channel Encryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 The TOE does not delete keys, given that these keys are part of the SSL protocol and are not accessible.
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/Channel Encryption The TOE does not delete keys, given that these keys are part of the SSL protocol and not accessible.
FDP_ACC.2/Local users	FDP_ACF.1	FDP_ACF.1/Local users
FDP_ACC.2/Domain users	FDP_ACF.1	FDP_ACF.1/Domain users
FDP_ACC.2/EMSCOMM user	FDP_ACF.1	FDP_ACF.1/EMSCOMM user

FDP_ACF.1/Local users	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/Local users FMT_MSA.3
FDP_ACF.1/Domain users	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/Domain users FMT_MSA.3
FDP_ACF.1/EMSCOMM user	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/EMSCOMM user FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1/Local users	None	
FIA_ATD.1/Domain users	None	
FIA_ATD.1/EMSCOMM user	None	
FIA_SOS.1	None	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	None	
FIA_UID.2	None	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2/Local users FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	None	
FTA_TSE.1/SEP	None	
FTA_TSE.1/MGT	None	
FTP_TRP.1	None	

FTP_ITC.1	None	
FRU_FLT.2	FPT_FLS.1	In failure, the operating boards in active state are switched with the stand-by boards which are continuously synchronized with the active boards. So the secure state is preserved.
FTP_TRP.1	None	

Table 10: Dependencies between TOE Security Functional Requirements

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 + ALC_CMC.4 and ALC_CMS.4 components as specified in [CC] Part 3+. No operations are applied to the assurance components.

Assurance class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**
Development	ADV_ARC	1
	ADV_FSP	3
	ADV_IMP	NA
	ADV_INT	NA
	ADV_SPM	NA
	ADV_TDS	2
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	4
	ALC_CMS	4
	ALC_DEL	1
	ALC_DVS	1
	ALC_FLR	NA
	ALC_LCD	1

	ALC_TAT	NA
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 Auditing

The TOE generates audit records for security-relevant events. (Please refer to FAU_GEN.1 for a list of event types, and the type of information recorded.)

The auditing functionality of the TOE cannot be started or stopped independently from the operational TOE. However, the TOE generates audit records for the start and shutdown of BSC6900, and of its individual subsystems. (FAU_GEN.1)

Where appropriate, the data recorded with each audit record includes the unique user ID associated with a subject during authentication. (FAU_GEN.2)

The logs are stored in a database that is used by the BSC6900 unit to store configuration and other data. No user can modify or delete these logs because all the accesses to the database are limited to the BSC6900 unit. (FAU_STG.1)

If the audit records stored in the logs exceed the defined limit such as 5GB, the TOE will overwrite the oldest logs and continue to record. (FAU_STG.3)

Users from the M2000 and WebLMT can review the audit records available in the database. The search functionality is based on time intervals, user IDs, interface, workstation IP, result, and command name (please refer to the FAU_SAR.3 requirement to check the different selection parameters). (FAU_SAR.1, FAU_SAR.3)

7.1.2 Digital signature

To address security issues, digital signature mechanism to ensure the legitimacy and integrity of the software packages are provided.

When packaged, the Software files will be digitally signed by Huawei's digital signature tool, the process is as follow:

1. For each component file in the package, message digest (using SHA-256 algorithm) will be calculated, and the result will be recorded in the file
2. The SHA checksums will be signed by Huawei's digital signature private key (RSA)
3. The package software file, SHA checksum files, and digital signatures files will be packaged together to produce the final package.
4. The package then will be signed by Huawei digital signature private key (RSA), and then the final digital signatures will be generated. Finally, all those (the final signature and the public key) will be released together with the software packages.

5. The software package of the BSC6900 and GBTS is downloaded first to the BSC6900. Then digital signature is verified once in the BSC6900 unit. If the digital signature verification went ok, the software package corresponding to the GBTS is transferred to the GBTS unit. Finally the GBTS unit verifies the digital signature before starting the installation.

   (FCS_COP.1)

7.1.3 Access control

The TOE controls which operations users can perform. The product considers three kinds of users:

- **Local users**: users that are managed by the BSC6900 and which information is stored inside the BSC6900. The local users are only enabled to access the BSC6900. There are users of BSC6900 with administration operational rights that creates and assigns operational rights to the local users in order to allow the execution to certain commands. The assignment of the operational rights is as follows:
  - · The users of BSC6900 are grouped by user groups (or roles).
  - · Then an administrator of BSC6900 assigns command groups to these user groups.
  - · The command groups contain the commands that are can be executed.

  Each time a local user logs in the BSC, the system gets the list of commands that the user can executes by following this assignment in order the perform the access control. (FDP_ACC.2/Local users, FDP_ACF.1/Local users, FIA_ATD.1/Local users, FMT_MSA.1/Local users)

- **Domain users**: these are users managed by the M2000 and can access different managed elements. The information about these users is stored in the M2000, so the BSC6900 cannot manage the operational rights from these users. The only management available from the BSC6900 for the domain users attributes is the password modification (for the domain user currently logged). So the creation and operational rights assignment of domain users is out of the scope of BSC6900. Each time a domain user logs in the BSC6900, the M2000 communicates the BSC6900 the commands that this user can execute. (FDP_ACC.2/Domain users, FIA_ATD.1/Domain users, FDP_ACF.1/Domain users, FMT_MSA.1/Domain users)

- **EMSCOMM user**: this is a built-in user of BSC6900 that is used by the M2000 to operate with the BSC. This user has permission to execute all the commands of BSC6900 and cannot be modified neither deleted. This user is only for the communication with M2000 and cannot access the TOE through other interfaces (cannot use WebLMT).(FDP_ACC.2/EMSCOMM user, FIA_ATD.1/EMSCOMM user, FDP_ACF.1/EMSCOMM user)

The TOE has pre-defined Command Groups, such as “Alarm Management Command Group” and “Performance Query Command Group”. These can be modified or deleted by authorized administrators, who can also create additional Command Groups to reflect operational needs.

Also, the BSC6900 unit of GBTS comes with 4 predefined user groups: Guest, User, Operator and Administrator. Also, there is another user group, “Custom”, which can be configured with the different command groups in order to get a different user group from those provided by the BSC6900. (FMT_SMR.1)

7.1.4 Authentication

The TOE offers different authentication methods depending on the kind of user. Every user must be authenticated before the execution of any command. The different authentication methods are:

Local users’ authentication: the authentication for local users is performed in the BSC6900 and based in user and password. The BSC6900 unit maintains all the security attributes for each local user in order to identify and authenticate the local users in the log in. (FIA_ATD.1/Local users)

Domain users’ authentication: the authentication of domain users is performed in the M2000 unit and based in user and password. The security attributes of the domain users are stored in the M2000. The BSC6900 asks the M2000 about the user permission to connect. Then, M2000 checks the domain user permissions about the managed elements he can connect to and communicates the result to the BSC6900. In affirmative case, the operational rights of the user are communicated to the BSC6900 when logged in in order to perform the access control. (FIA_ATD.1/Domain users)

EMSCOMM user authentication: this user is related with the execution of commands from the M2000 and represents to a second user who is operating in the M2000 and managing configuration data of the BSC6900. The authentication of this user is performed only once, and it is understood as the connection between the M2000 and the BSC6900 when this is inserted in the management network. The connection follows a special arithmetic private for each party and, once performed, it remains alive until disconnection, so no further connections are needed each time a MML command is executed. This is a built-in user of the BSC6900, so his information is stored within the TOE. (FIA_ATD.1/EMSCOMM user)

(FIA_UAU.5)

The BSC6900 enforces timer-based account lockouts; administrators can specify after how many consecutive failed authentication attempts an account will be temporarily locked, and whether the counter for failed attempts will be reset automatically after a certain amount of minutes. (FIA_AFL.1)

Authorized administrators are able to configure a system-wide password policy that is then enforced by the TOE. Besides the minimum length of the password, which can be set to be between 6 and 32 characters, administrators have the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters). (FIA_SOS.1)

The TOE can identify administrators in the management network by a unique ID and enforces their identification before granting them access to the TSF management interfaces. Warning of “error username or password” will be prompted when the user fails to provide a correct username or password. (FIA_UID.2)

Authentication based on user name and password is enforced prior to any other interaction with the TOE for all external interfaces of the TOE, typically via the WebLMT, used by administrator. (FIA_UAU.2)

If applicable, i.e., if an administrator has specified values for these parameters for a specific user, the TOE will deny authentication of the user if the user tries to authenticate in a timeframe that lies outside of the “login start time” and “login end time” specified for the user. When the user uses an expired password to login, the system must request the user to modify the password. The TOE also provide login time control mechanism: Each account can be configured with the login time segment, including the valid date range, time segment, and week restriction. Any login is prohibited beyond the configured time segment. (FTA_TSE.1/MGT)

After the user login, if user account is not locked after the departure of long time is likely to be attacked; the TOE will lock the account to prevent the account information from being leaked. And the user must login again. (FTA_SSL.3)

7.1.5 Fault Tolerance

The TOE presents a backup board in stand-by mode of operation for the OMU and Interface boards. In case of failure a switchover between the boards is performed. This way, the performance and availability of the TOE remains the same. (FRU_FLT.2)

In order to import the more appropriate configuration data for the new switched boards, the TOE provides the functionality to export and import this configuration data to/from the BSC6900 machine or to/from an external user machine. (FDP_ITC.1)

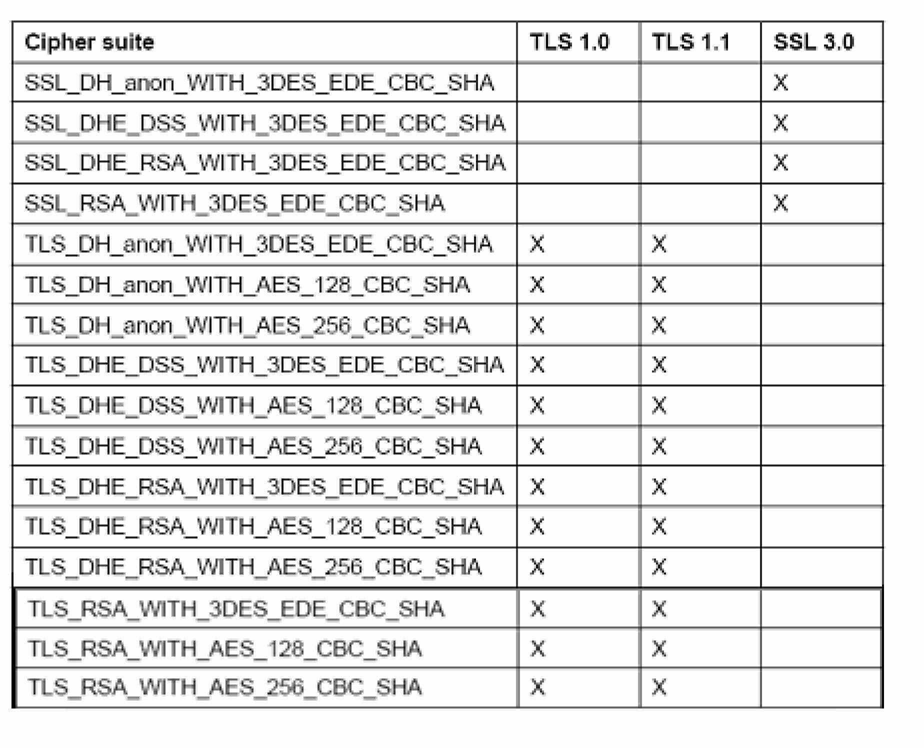
7.1.6 Communications security

The TOE provides communications security for network connections to the OMU. This includes connections via the following interfaces:

1. OM connections (include MML, BIN, FTP connections) between M2000/WebLMT and the BSC6900 (using SSL/TLS) (FTP_TRP.1)

2. HTTPS connections between WebLMT and the BSC6900 (using SSL/TLS) and FTPS between the operational environment and the BSC6900 (using SSL/TLS)

3. The SSL/TLS cipher suites supported for SSL connections are:



Cipher suite	TLS 1.0	TLS 1.1	SSL 3.0
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA			X
SSL_RSA_WITH_3DES_EDE_CBC_SHA			X
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_128_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	X	X	
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_RSA_WITH_AES_256_CBC_SHA	X	X	

The TOE and the M2000 agree on a randomly generated AES session key that is exchanged in an AES-encrypted message using a FixKey, a static key configured by administrators via the WebLMT interface and stored in the TOE's configuration database.

Also, during the authentication of a domain user, the BSC6900 communicates with the M2000 in order to perform the identification and authentication.

(FTP_TRP.1, FCS_COP.1/Channel encryption.1 and FCS_CKM.1)

7.1.7 Resource management

The TOE provides VLAN to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead.

The TOE support VLAN division based on flows such as signalling flows, data flows, or management flows. In other words, different VLAN tags are marked on the three types of flows and they are separate from each other.

The VLAN functionality is implemented in the both units of the TOE, the BSC6900 and the GBTS, in order to control the connection between them.

The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE which might cause system overload and service interruption.

The IP-based Access Control List provides a simple security policy that controls the incoming and outgoing data of unauthorized users. The IP-based Access Control List determines what data is allowed to enter the transmission port and what data is not allowed to enter the transmission port. In this way, the ACL filters the illegitimate data.

The IP-based Access Control List controls the network access, preventing the network attacks. In addition, the IP-based Access Control List filters out illegitimate data flows, improving the network performance.

The IP-based Access Control List consists of multiple rules. Each rule contains the following filtering conditions:

1. Protocol type (ICMP, TCP or UDP,,)
2. Source IP address and mask
3. Source port
4. Destination IP address and mask
5. Destination port
6. ACL Action (Drop, Permit)

(FTA_TSE.1/SEP)

7.1.8 Management of TSF

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes:

1. User management, including User Group memberships, passwords, account lockout, validity periods for an account and/or password, etc.

2. Access control management, including the definition of Command Groups, and the association of users and User Groups with Managed Elements, and Command Groups in Manage Authority and Operate Authority relationships.

3. Enabling/disabling of SSL for the communication between WebLMT, M2000, BSC6900 and GBTS.

4. Configuration of VLAN for the different plane between the TOE environment, the GBTS and the BSC6900.

5. Configuration of Role_based Access Control List for the communication between the TOE environment and the TOE.

6. All of these management options are typically available from the WebLMT GUI and the M2000 GUI.

(FMT_SMF.1)

The creation of new local users in the TOE is implemented in such a way the new user is assigned to the Guest user group as default value. This assignment can be modified during the creation by the administrator to state the appropriate assignments. (FMT_MSA.3)

8 Abbreviations, Terminology and References

8.1 Abbreviations

MSC	Mobile Switch Center
MBSC	Multimode Base Station Controller
BTS	Base transceiver station
SGSN	Serving GPRS Support Node
OSS	Operating Support System
CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
LMT	Local Maintenance Terminal
RMT	Remote Maintenance Terminal
AIU	Advanced Interface Unit
CLI	Command Line Interface
GUI	Graphical User Interface
SSH	Secure Shell
SSL	Secure Sockets Layer
PIU	Packet Interface Unit
OMU	Operation & Maintenance Unit

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE’s point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

Operator See User.

User: A user is a human or a product/application using the TOE.

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. July 2009. Version 3.1 Revision 3.

[CEM] Common Methodology for Information Technology Security Evaluation. July 2009. Version 3.1 Revision 3.