BUSINESS UNIT :	*Terrestre, Navale e Satellitare*	**CAGE CODE:**	A0069
TIPO DOCUMENTO: *DOCUMENT TYPE*	CC EVALUATION DELIVERABLE	**COMPOSTO DI PAGINE:** *COMPOSED OF PAGES*	80
TITOLO: *TITLE*	MPS1xx SECURITY TARGET	**CODICE:** *CODE*	6ti-sd000001-e
		Ediz.: *ISSUE*	**07**
		DATA): *DATE (dd/mm/yy)*	**JUL 26TH 2004**
PROGRAMMA: *PROGRAM*		**PROGETTO:** ***PROJECT***	MPS1xx SWITCH
RIFERIMENTI CONTRATTO *CONTRACT REFERENCE*	- **CLIENTE:** *CUSTOMER* - **CONTRATTO:** *CONTRACT* - **CDRL N°:**		

Preparato da *Prepared by*	**Nome** *Name*	**Firma** *Signed*
FUNZIONE *DEPARTMENT*	Paolo Cassissa Roberto Moscolin Roberto Mozzone Stefano Pinna	
Approvato da *Approved by* **FUNZIONE** *DEPARTMENT*	Giancarlo Zunino	
Approvato da *Approved by* **FUNZIONE** *DEPARTMENT*		
Autorizzato da *Authorised by* **FUNZIONE** *DEPARTMENT*		
Autorizzato da *Authorised by*		

FUNZIONE *DEPARTMENT*		

REVISIONI DELLE PAGINE (Pages Revision)										
PAGINE *(Pages)*										**0**
0										
10										
20										
30										
40										
50										
60										
70										
80										
90										
100										

CLASSIFICAZIONE DELLE PAGINE (classification sheet)	
0	Pagine **SEGRETO** *(Pages Secret)*
0	Pagine **RISERVATISSIMO** *(Pages confidential)*
0	Pagine **RISERVATO** *(Pages Restricted)*
75	Pagine **NON CLASSIFICATO** *(Pages Unclassified)*
75	Pagine **TOTALE** *(Total Pages)*

REGISTRAZIONI REVISIONI

(Revisions Record)

Ed. *(Issue)*	**Change Request** *(C.R.. n°)*	**Data** **(***Date)*	**Storia delle revisioni** *(Revisions History)*
1	CR-t/03/000248	7Apr03	Prima emissione/ First issue
2	CR-t/03/000249	29Jul03	As per CLEF OR2/1-OR2/11 and OR4/1-OR/4
3	CR-t/03/000290	3Nov03	1. As per CLEF OR2/12-OR2/19 and OR4/5-OR/7Crypting of Secrets (rev. id. REV.1)
4		11Nov03	2. "Security" Manager Role removed (rev. id. REV.2) 3. "Lockout Admin" Manager Role inserted with associated Manager Role scope (rev. id. REV.3) 4. PVC and sPVC Connection management (rev. id.REV.4) 5. Gateway management (rev. id.REV.5) 6. Refinement in Self-Affiliation Facility for the management of possible multiple presence of a Subscriber users in the connected network (rev. id.REV.6) 7. Scope Query 03/10/03 (rev. id. REV.7) 8. Editing and inconsistence error from previous issues (rev. id. REV.8)
5	CR-t/04/000100	9Apr04	As per CLEF OR4/11, OR4/13, OR4/16, OR2/22, OR2/23
6	CR-t/04/000221	31May04	As per CLEF OR2/26 plus editing errors
7	CR-t/04/000298	26Jul04	As per CLEF review

LISTA DI DISTRUBUZIONE *(Distribution List)*	
	Destinatario/Funzione *(Address/Function)*
Interna *(Internal)*	**Questo documento e' disponibile nel Sistema Informatico della Società.** **La validità delle copie, sia in formato elettronico che cartaceo, dovrà essere verificata sul Sistema, prima del loro utilizzo**. **This document is available in the Company's Data Management System.** **The validity of copies, whether electronic or paper, shall be verified on the System before their use.**
	Cliente *(Customer)*
Esterna *(External)*	

Preparato da: *Prepared by*		**Sede Legale:** *Head Office*	
Paolo Cassissa *Roberto Moscolin* *Roberto Mozzone* *Stefano Pinna*	MARCONI SELENIA Communications S.p.A. SITE:		MARCONI SELENIA Communications S.p.A. Via A. Negrone, 1/A 16153 Genova ITALY

PUNTO DI CONTATTO: *Point of contact*	Per informazioni relative a questo documento rivolgersi a *Any questions arising from this document should be addressed to*		
NOME *NAME*	**FUNZIONE** *FUNCTION*	**TELEFONO** *TELEPHONE*	**FAX** *FAX*

INDICE

(index)

INDEX OF TABLES

1. SECURITY TARGET INTRODUCTION

This section provides identifying information for the MPS1xx Switch Security Target (ST), by identifying information regarding the Target of Evaluation (TOE).

1.1 SECURITY TARGET NAME

This document specifies the Security Target for MPS1xx Switch.

1.2 TOE IDENTIFICATION

MPS1xx switch family includes a complete range of products designed to provide broadband switching services to support military networks in both tactical and strategic environments.

For the purpose of this document MPS1xx switch refers two different models:

Switch Model	Versions	Description
MPS 115	V 1.4 pack 2[1]	6 rack Units height mechanics, with 14 card slots that can be differently equipped
MPS145	V 1.4 pack 2	3 rack Units height mechanics, with 6 card slots that can be differently equipped

Table 1: MPS1xx Model referred in ST

1.3 EVALUATION ASSURANCE LEVEL

Assurance claims conform to EAL4 + (Evaluation Assurance Level 4 plus Augmented Component Flaw Remediation) from the Common Criteria Version 2.1, August 1999 (ISO/IEC 15408).

1.4 SECURITY TARGET OVERVIEW

This ST describes the objectives, requirements and rationale for the MPS1xx Switch. The language used in this Security Target is consistent with the Common Criteria for Information Technology Security Evaluation, Version 2.1 (ISO/IEC 15408).

Based on an ATM core MPS1xx switches provide enhanced inter-working features that allow their deployment in multi-protocol networks, where it is possible to harmonize together ISDN, IP/LAN and legacy STANAG/EUROCOM systems.

MPS1xx switches provide shared transport services on narrow and wide band bearers, of either good or poor quality in relation to BER and propagation delays. Dynamic band allocation features, the delivery of QoS to the different data and voice applications, a rugged design, the availability of platform versions and full control capabilities complete the profile of this family of products.

The MPS1xx can be either introduced seamlessly in legacy systems or be deployed in any new scenario to serve the requirement of modern Armed Forces, at any command echelon and for any mission.

[1] The software release and hardware part types equipped are the same for both Models

1.5 CC CONFORMANCE CLAIM

The MPS1xx switch is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL4 conformant.

1.6 GLOSSARY

AC	Access Control
ACP	Access Control Policy
ATE	Analysis of Testing
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
CC	Common Criteria
CM	Configuration Management
CMP	Configuration Management Plan
EAL	Evaluation Assurance Level
FSP	Functional Specification
HL	Higher security Level
HLD	High Level Design
IEC	International Electrotechnical Committee
IFCP	Information Flow Control Policy
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Standard Organization
IT	Information Technology
ITU-T	International Technical Union-Technical
LAN	Local Area Network
LL	Lower security Level
LLD	Low Level Design
MLS	Multi Level Secure
MPS	Multi Protocol Switch
MPS1xx	MPS115 and MPS145
NNI	Node-Network Interface
NSW	Non-Secure Warning
PDH	Plesiochronous Digital Hierarchy
PIN	Personal Identification Number
PP	Protection Profile

PVC	Permanent Virtual Circuit
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SF	Security Function
SFA	Security Functional Analysis
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
SPM	Security Policy Model
sPVC	Soft PVC
ST	Security Target
Stanag	NATO Standardization Agreement
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
UG	User Guidance
Uni	User Network Interface
VA	Vulnerability Assessment
WAS	Wide Area System

1.7 GENERAL DEFINITIONS

The following definitions are of general scope and will be referred throughout the ST document as Keywords (in capital letter), as well as the rest of Evaluation documents.

Product	The collection of hardware and software part comprising MPS115 and MPS145
Management Interface	The dedicated management port used for management purposes. It may refer both the TOE serial interface and TOE Ethernet interface
Access Interface	Local traffic channel managed by the TOE. Access Interfaces consist of local channels used by TOE-registered subscriber to access TOE switching facilities
Trunk Interface	Transmission link interface between two TOEs
Gateway Interface	Transmission link interface between the TOE and another IT product that is outside the scope of Information Flow Control Policy
Traffic Interface	An Access, Trunk or Gateway Interface
Card Failure	A failure condition detected by TSF at TOE card level
Network Failure	A failure condition detected by TSF at Trunk Interface level
Management Data	The subset of the entire user data maintained by the TSF that is security relevant for the enforcing of SFPs. These include both security attributes (e.g. Subscriber Security Level) and TSF data (e.g. audit records). Changes to Management Data may result from explicit action by authorized Manager user or by any other TSF-mediated actions (e.g. Subscriber Self-affiliation).
Accounting Data	The subset of Management Data that will be maintained by TSF in order to manage security attributes related to the accounting process of Subscriber and Manager users
Permanent Data	The subset of Management Data that are not lost as a consequence of a power-off event occurred at the TOE
Manager Roles	The following roles are defined for the enforcing of Access Control SFP: • **"Operator"** • **"Manager"** • **"Global"** • **"Lockout Admin"**
Registered User	A TOE user, active inside the TOE security boundary, that is uniquely recognized by the TSF as a consequence of the permanent association between that user and a set of security attributes expressed in terms of Management Data; Registered Users comprise ISDN Registered Users that access the TOE via an ISDN S0 or ISDN E1 link, IP Network Registered Users that access the TOE via a standard IP link and ATM Registered Users that access the TOE via a standard ATM User-Network Interface; ISDN and ATM Registered Users are uniquely characterized by an address specified in the space and format defined by the TOE numbering plan; IP Network Registered Users are identified instead by means of the shared IP address associated to the sub-network they belong to
Subscriber User	A Registered User that is capable of accessing the TOE switching facilities; in order to access the TOE switching facilities a Subscriber user must be bound to an Access Interface; ATM and IP Registered Users are statically bound to Access Interfaces, while ISDN Registered Users are bound to Access Interfaces by means of Affiliation Facility

Affiliation Facility	A security relevant facility provided by the TOE in order to bound an ISDN Registered User to an Access Interface; by means of Affiliation Facility an ISDN Subscriber User is not statically associated to a specific Access Interface. In order to access the switching facility the Subscriber, if capable, can self-affiliate at that TOE connecting his phone terminal to a suitable Access Interface, dialling the self-affiliation facility code, his associated Personal Identification Number (PIN) and phone number. Alternatively an explicit action by a Manager user is required in order to make the Subscriber affiliated at the TOE. Because of the change of Management Data as a consequence of successful result of the self-affiliation facility, Access Control SFP mediates Self-affiliation Facility. A Subscriber in affiliated status can be de-affiliated by an explicit action from Manager user or entering the De-affiliation Facility code, his associated Personal Identification Number (PIN) and phone number.
Gateway	A logical point of interconnection across a Gateway Interface between a far-end IT entity outside of the TOE security boundary and the TOE itself
Route	A concatenation of multiple paths joining two TOE Traffic Interfaces at the same node or at different nodes across the network. The TOE establishes a Route during call set up process and generally consisting of Trunk Interfaces, the TOE itself and the Access or Gateway Interfaces at which Subscribers or Gateways respectively are connected
PVC Connection	A switched connection between two TOE Traffic Interfaces at the same node that is not lost as a consequence of a power-off event occurred at that TOE
sPVC Connection	A switched connection between two TOE Traffic Interfaces at different nodes that is not lost as a consequence of a power-off event occurred at one or both of the TOEs or a failure in one of the transmission path comprising the Route between the two nodes in the network
(s-)PVC Capable Interface	A Traffic Interface that is capable of supporting PVC and/or sPVC Connection
Subscriber user data	Data created by and for the Subscriber user that does not affect the operation of the TSF.
Gateway Data	Data created by and for an entity associated to Gateway that does not affect the operation of the TSF
PVC Connection Data	Data created by and for the PVC Connection that does not affect the operation of the TSF
sPVC Connection Data	Data created by and for the sPVC Connection that does not affect the operation of the TSF
Conference Facility	A security relevant facility provided by the TOE by which a Subscriber User can be dynamically added to other predefined Subscribers as a party in a multipoint-to-multipoint connection. The same Subscriber can be dynamically removed as a party from the provisioned connection. Information Flow Control SFP mediates Conference Facility
Security Level	A security attribute associated to Subscriber, Gateways, TOE Traffic Interfaces and switched calls between Subscribers, Gateways, PVC and sPVC Connections. TSF is capable of managing up to 5 Security Levels plus a security bottom level corresponding to non-secure traffic conditions
Non-Secure Warning	A Subscriber equipped with suitable terminal equipment shall be provided by

the TSF with Non-Secure Warning indication when involved in a call established with a Security Level lower than the Subscriber Security Level. The type of Non-Secure Warning indication provided depends on the type of Subscriber terminal equipment. It may consists in a tone mixed with the normal voice traffic and/or a display indication

Downgradeable Subscriber A Subscriber which supports the capability of adapting the statically associated Security Level to the actual security level of an established call: in this case the Subscriber is referred as Donwgradeable Subscriber and the condition will be indicated with the symbol "⇓"; on the contrary, the symbol "⇔" indicates the fact that Subscriber may not be downgraded

Downgradeable Gateway A Gateway which supports the capability of adapting the statically associated Security Level to the actual security level of an established call: in this case the Gateway is referred as Donwgradeable Gateway and the condition will be indicated with the symbol "⇓"; on the contrary, the symbol "⇔" indicates the fact that Gateway may not be downgraded

Downgradeable PVC Connection A PVC connection which supports the capability of adapting the associated Security Level to the Security Level of the TOE Traffic Interfaces involved in the connection

Downgradeable sPVC Connections An sPVC connection which supports the capability of adapting the associated Security Level to the Security Level of the TOE traffic Interfaces involved in the connection

Secure Capable Entity An IT entity defined outside of the TOE security boundary that is capable of carrying security relevant information at a Gateway Interface

Secure Uncapable Entity An IT entity (e.g. an IT Product) defined outside of the TOE security boundary that is uncapable of carrying security relevant information at a Gateway Interface

Security Differentiator A security attribute associated to a Gateway Interface and used for the mapping of the security features of the calls received/sent from/to a Secure Capable Entity: for incoming calls across the Gateway Interface the Security Differentiator is used in combination with the information extracted from the external signalling flow in order to set the security level and downgradable capability of the call offered to the TOE; for outgoing calls across the Gateway Interface the Security Differentiator is used in combination with the information extracted form the internal signalling flow in order to discriminate whether the resulting call is to be offered with an overall secure or non-secure feature to the Secure Capable Entity

2. TOE DESCRIPTION

This section provides background information, the TOE functionality and desired security capabilities for MPS1xx Multi-Level Secure/Multi-Protocol Switch environment.

MPS1xx family caters for different equipment configurations, differing in terms of mechanical dimensions, connectors (military or civilian), capacity, etc. and suitable, depending on the configuration, for tactical or strategic applications.

MPS115 is characterized by 14 card slots that can be differently equipped.

MPS145 is characterized by a 6 card slots that can be differently equipped. It is based on the same hardware and software components of the MPS115.

2.1 TOE COMPOSITION

The evaluated configuration consists of the collection of all the hardware and software components that comprise the TOE and is identified by a TOE Version which coincides with the evaluated Product Release.

The following MPS115 hardware parts (and associated part-number) are included in the evaluated configuration:

- Wired Cover Assembly (144-4118/01.01)
- Blank Panel Netmod (341-4706/01.01)
- Blank Panel MSM (341-4707/01.01)
- 24/28V Power Supply Unit (141-6083/01.01)
- 110/220V Power Supply Unit (141-6082/01.01)
- MSM Unit (141-6081/11.01)
- 4 x 155 Mbps ATM Optical Unit (141-6084/01.01)
- 3 x N Mbps ATM FEC Unit (141-6175/01.01)
- 4 x 2 Mbps ISDN E1T1 Unit (141-6222/01.01)
- 4 x 2 Mbps EUROCOM Unit (141-6223/01.01)
- 16 x S0 ISDN Unit (141-6272/01.01)
- 8 x (10/100 Mbps) IP Unit (141-6087/01.01)

The following MPS145 hardware parts (and associated part-number) are included in the evaluated configuration:

- Wired Cover Assembly (143-4154/03.01)
- Blank Panel (341-4769/01.01)
- AC/DC Power Supply Unit (141-6191/01.01)
- MSM Unit (141-6187/11.01)
- 4 x 155 Mbps ATM Optical Unit (141-6186/01.01)
- 3 x N Mbps ATM FEC Unit (141-6209/01.01)
- 4 x 2 Mbps PRI ISDN Unit (141-6249/01.01)
- 4 x 2 Mbps EUROCOM Unit (141-6250/01.01)

- 16 x S0 ISDN Unit (141-6273/01.01)
- 8 x (10/100 Mbps) IP Unit (141-6188/01.01)

The following MPS software components are included in the evaluated configuration:

- MPS Software Release 1.4 pack 2

2.2 TOE FUNCTIONALITY

MPS1xx switch design is compliant with ITU-T and ATM Forum Recommendations with additional features (such as support for narrow-band links, cell hardening against high BER links, priority, and security) that are essential in military networks.

It supports a large set of ATM (UNI/NNI) and InterWorking interfaces to provide integration of user and network services when connected to existing circuit-oriented military and civil communication systems. Full backward compatibility to STANAG/Eurocom networks is maintained. When arranged in WAS networks, the switch can operate with saturation routing, on either civil (PDH and SDH) or military bearers, with or without the cell hardening facility.

Many different numbering plans can be implemented, either in accordance with the major reference standards or customized to specific user needs.

The switch can be equipped with digital subscribers cards to get the maximum level of functional and mechanical integration.

The switch can be locally or remotely managed and all the operating parameters can be changed on the fly to meet mission specific requirements. Powerful self-diagnostics greatly ease the field maintenance task. The mechanical construction and environmental performance of the switch allow different types of installation, e.g. in sheltered mobile stations for strategic infrastructure networks, or in air-transportable packages.

The MPS1xx series can be managed locally using a RS232 Serial Interface or by means of a Network Management System using a 10 BaseT Ethernet interface.

Node management through Serial interface requires a VT100 compatible video terminal, or Personal Computer running terminal emulator software located close to the switch.

Ethernet Interface allows the MPS1xx series to be managed by means of a Network Management System not physically adjacent to the node.

There are different roles in the management of nodes. All personnel in management roles are assumed to be trusted at some level.

The management facility is a privileged access area with only the network management employees having access privileges.

The equipment can be configured, depending on the various needs, as either an access node or a trunk node, thus providing the greatest operational flexibility.

As an access node the switches can interface ATM subscribers both at low-medium bit rate (2, 8, 34, 45 Mbit/s) and at high bit rate (155 or 622 Mbit/s). Additionally, it can be equipped with Subscriber Access Units that allow connections to ISDN switches, ISDN users, LANs and 2 Mbit/s cross-connected subscribers.

It is also possible to connect the MPS1xx switch to digital switches compliant with EUROCOM D/1 Specs, via a EUROCOM multichannel interface unit at 16, 32 or 64 channels, with a sampling rate of 16 or 32 Kbit/s.

Similarly, the MPS1xx series can be connected to both EUROCOM and NATO Military Networks via a EUROCOM or STANAG multichannel digital gateway.

The MPS1xx series can interface other equipment of the same type using ATM trunk connections either at low-medium rate (32, 64, 128, 256, 512 Kbit/s, 1, 2, 8, 34, 45 Mbit/s) or at high rate (155 or 622 Mbit/s).

Finally, the MPS1xx series can interface ISDN Networks via standard E1 links and provided with ISDN S0 interfaces.

The equipment can operate from an internal timing source, from a high stability external one or from a clock derived from an interface.

Either a local or remote operator via a local or remote Network Management System can manage the equipment.

2.3 NETWORK SCENARIOS

The MPS1xx switch is designed for tactical use and it provides a set of characteristics in terms of mechanics, connectors, security and protocols that make the switching suitable for such employment.

The equipment, with the relevant connectors and mechanics, is also available, suitable for strategic applications as it is able to interface ATM, IP, ISDN and STANAG/EUROCOM standard equipment.

The general characteristics for the MPS1xx switch in Tactical or Infrastructure Scenarios are described in the following paragraphs.

2.3.1 TACTICAL SCENARIO

In a Tactical Scenario the equipment is installed in shelters or used directly in the field. The shelters are deployed in the field and, typically, interconnected with radio relay on poorly engineered links, with consequent high BER and a limited transmission capacity.

When the shelters are close enough together fiber optic connections may be used. Shelters may subsequently be moved due to new operational requirements.

The users can move inside such a deployed network and use different switching nodes, affiliating with the closest switching node as necessary.

Considering the above the Tactical Scenario is characterized by:

- Ability to operate in a critical environment in accordance with tough operational requirements
- Use of several kinds of transmission media
- Use of low bit rate bearers
- High BER on radio links, due to both scarce link engineering and enemy’s jamming
- Rapid deployment on the field
- Capability of reconfiguration and support of the user’s mobility
- Communications security and selective access to network resources
- High fault resilience with maintenance of a service grade proportional to the damage suffered

The following depicts the use of MPS1XX switch in a typical tactical scenario:

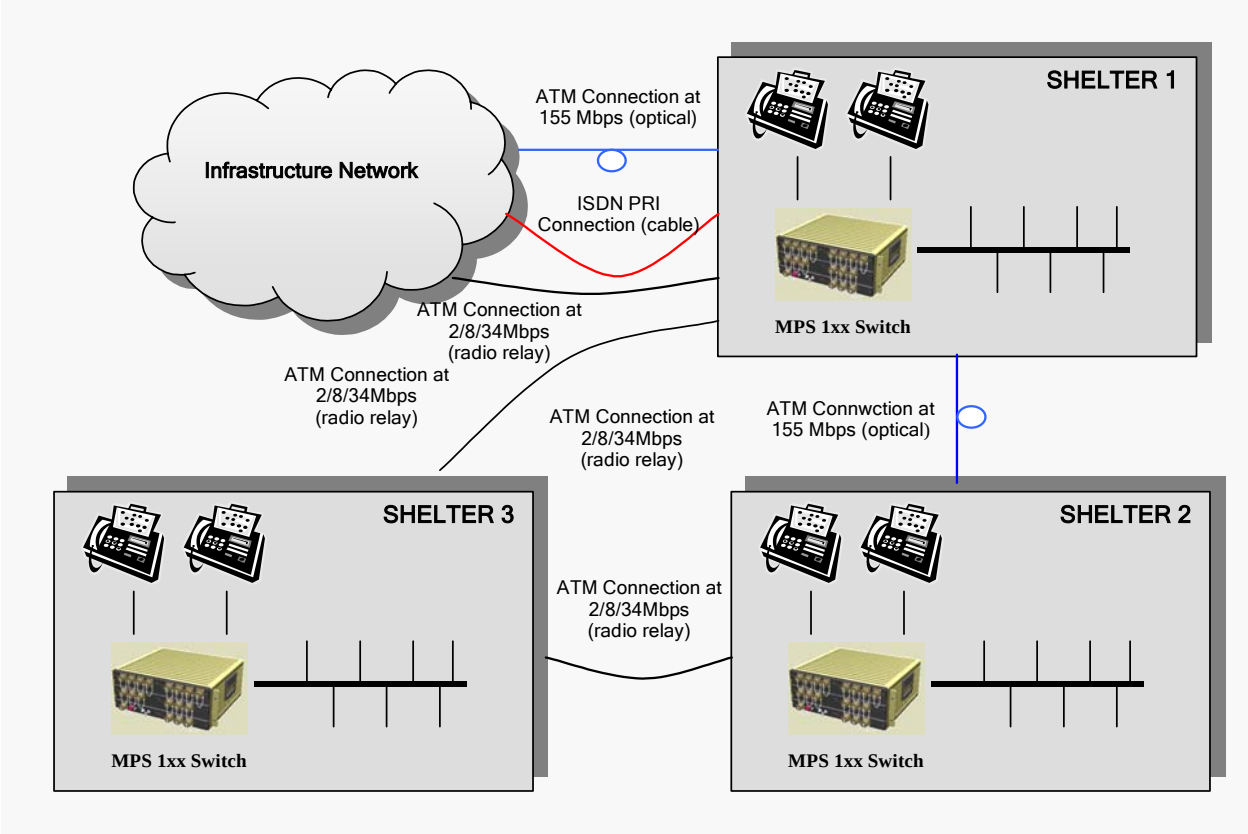

Figure 1: Example of Tactical Scenario

2.3.2 STRATEGIC SCENARIO

In a Strategic Scenario the equipment is installed in fixed emplacements (buildings) and the interconnections between different sites are made by means of radio relay (with a capacity of 34 Mbit/s or 155 Mbit/s) or by means of fiber optic cables (with a capacity of 155 Mbit/s or 622 Mbit/s).

In such a context there is a limited mobility of the network in terms of movement of the emplacements. It remains the requirement, for a user, to be able to move inside the network connecting from time to time to the closest switching node, maintaining its own particular characteristics (as defined in the user profile) in terms of priority, services, barring, etc.

From the above it follows that the Infrastructure Scenario is characterized by:

- Fixed Installations
- Medium-High Bit Rate Transmission Media
- Low Bit Error Rate
- Civilian Standards for interfacing to Private Networks
- Interoperability with Tactical Systems
- (Naval Networks are also similar to Strategic Networks)

The following depicts the use of MPS1XX switch in a typical infrastructure scenario:

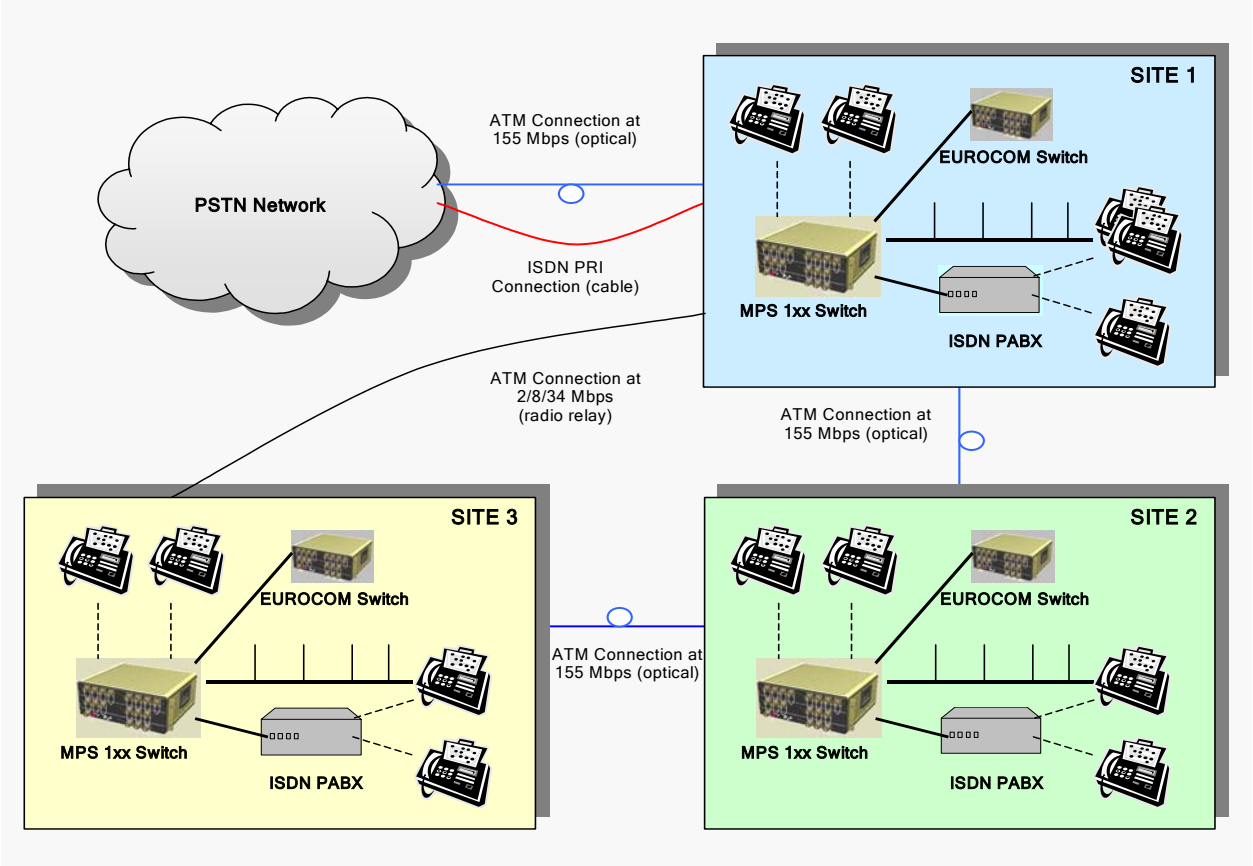

Figure 2: Example of Strategic Scenario

2.4 TOE SECURITY FUNCTIONALITY

The TOE, intended as the Product in the evaluated configuration, when properly installed in the deployed network, in the respect of the environmental assumptions and its intended usage and for the scope limited to its security boundaries as defined per Gateway Interfaces, implements the following security functionality:

- Access Control Policy for all the security relevant information based on Manager user identification and authorization information
- Information Flow Control Policy for all incoming and outgoing Subscriber user and Gateway traffic flows, based on Multi-Level-Secure and System-High capabilities associated to each Subscriber user and Gateway profile
- Information Flow Control Policy for all incoming and outgoing traffic flows associated to PVC and sPVC Connections between two (s-)PVC Capable Interfaces
- Supporting of a well-defined mapping rule between the traffic flows outside of the TOE security boundary and the traffic flows inside the TOE security boundary, in accordance with Information Flow Control Policy rules, both for Secure Capable Entity and Secure Uncapable Entity connected at Gateway Interfaces
- Intrusion detection and prevention, keeping separate security relevant management information from traffic flows and keeping separate the different Subscriber user, Gateway, PVC and sPVC Connections traffic flows one from the other.

- Auditing capabilities for all the security relevant events
- Secure fault management based on automatic failure detection and recovery

3. TOE SECURITY ENVIRONMENT

3.1 SECURE USAGE ASSUMPTIONS

3.1.1 PHYSICAL ASSUMPTION

A.SECURE_ENVIRONMENT

In order to protect both Manager, Subscriber user, Gateway, PVC and sPVC data from malicious modifications, the TOE shall be installed and maintained in a secure environment.

3.1.2 PERSONNEL ASSUMPTIONS

A.ADMIN_COMPETENT

TOE Administrators are competent to carry out administration of the TOE, understand the consequences of their actions and the Security Policies in place, and advise every TOE user of the usage requirements.

A.ADMIN_DOCS

TOE Administrators will follow all policies and procedures described in the TOE system documentation to ensure secure administration of the TOE.

A.ADMIN_NOEVIL

As the security functions of the TOE can be readily compromised by authorised administrators, it is assumed that they will have successfully completed a security background check before being granted access to the TOE management functions and are assumed to be non-hostile and can be trusted to do their duties correctly.

3.1.3 CONNECTIVITY ASSUMPTIONS

A.NETWORK_FRAGMENT

A network management policy must be defined for the control of network fragments as MPS will do nothing to prevent multiple affiliations in different (non-communicating) network fragments which are then connected together.

A.TRUSTED_GATEWAY

Gateway Interfaces of the TOE will be connected to non-hostile and trusted IT entity, both Secure Capable and Secure Uncapable, defined outside of the TOE security boundary

3.2 TOE INTENDED USAGE ASSUMPTION

A.POWER_SUPPLY

Network deployment must ensure that the MPS is provided with both battery and mains electrical power supply.

A.RELIABLE_TIME_STAMP

A network management policy must be defined for the initial setting of correct date and time in such a way that reliable time stamps support can be initialized in a proper way

3.3 THREATS TO SECURITY

The assets threats for those Security Objectives have been defined are:

- Security relevant information maintained by the TOE and referred as Management Data
- User Data consisting of Subscriber user data, switched at the TOE, and associated signalling information terminated at the TOE and processed by the call control algorithm
- Gateway Data resulting from the successful mapping between traffic flows outside of the TOE Security Boundary and traffic flows inside the TOE Security Boundary and associated signalling information
- PVC and sPVC Connection between (s-)PVC Capable Interface Data and associated signalling information
- User Data consisting of signalling information coming from a remote trusted IT product, terminated at the TOE and processed by the routing algorithm
- TOE implementation (i.e. executable code)
- TOE hardware parts (i.e hardware components)

In the following the term “TOE user” refers to any individual, which is active in the Operational Environment and may potentially access the TOE.

TOE users that have been assigned the capability of accessing Management Data and involved in Administration functions are qualified and referred as “Manager users”.

TOE users that have been assigned the capability of accessing TOE switching facilities are qualified and referred as “Subscriber users”.

TOE users that have not been assigned any capability (nor Managers or Subscribers), must be considered as “unauthorized users”: in this case TOE users are referred as unauthorized Managers and unauthorized Subscribers.

Authorized Manager users, authorized Subscriber users and unauthorized users, as defined above, represent human threat agents, while accessing Management Interface, TOE Traffic Interface during normal operations.

Moreover failure events that may randomly occur in hardware components of the TOE during normal operations, represent not-human threat agents.

T.Attack: Compromise of Information

An undetected compromise of information may occur as a result of an attacker (whether an authorized Manager and Subscriber user or not) attempting to perform actions that the individual is not authorized to perform.

T.Audit_Corrupt: Audit Data Corruption

Unauthorized Manager may tamper with audit data or unauthorized Manager users may cause audit data to be lost due to failure of the system to protect the audit data.

T.Breach: Transmission without Protection

A Subscriber user may either deliberately or accidentally attempt to transmit confidential information without appropriate protection measures in place.

T.Fail: Component or Power Failure

Failure of one or more system components or a power failure results in the loss of system-critical functionality and system data.

T.Unauth_Mgmt_Access: Unauthorized Access

An unauthorized Manager may gain access to system data due to failure of the system to restrict access.

The following puts in correspondence assets, threat, threat agents and methods of attack in terms of TOE interface from where the attack is conducted:

Asset	Threat	Threat Agent	Type	TOE Interface
Management Data	T.Attack	Authorized Manager	Erroneous action	Management Interface
Management Data	T.Attack	Authorized Subscriber	Erroneous action Malicious Action	Access Interface Trunk Interface Gateway Interface
Management Data	T.Attack	Unauthorized user	Malicious action	Management Interface Access Interface Trunk Interface Gateway Interface
Subscriber User Data Gateway Data PVC and sPVC Data	T.Attack	Authorized Manager	Erroneous action	Management Interface
Subscriber User Data	T.Attack	Authorized Subscriber Unauthorized Subscriber	Malicious action	Access Interface Trunk Interface Gateway Interface
Management Data	T.Unauth_Mgmt_Access	Unauthorized Manager	Malicious action	Management Interface
Management Data	T.Audit_Corrupt	Unauthorized Manager	Malicious action	Management Interface
Subscriber User Data Gateway Data PVC and sPVC Data	T.Breach	Authorized Subscriber Unauthorized Subscriber	Malicious action	Access Interface Trunk Interface Gateway Interface
TOE hardware parts	T.Fail	Failure event	Random	N.A

Table 2: Assets, threat, threat agent, methods of attack

3.4 ORGANISATIONAL SECURITY POLICIES

P.Audit_Review: Audit Review

Audit information is reviewed and analysed on a periodic basis in accordance with the security policy.

P.Default_Config: Default Configuration

The default configuration settings for the TOE will have all functions that weaken or break TOE security functions disabled. All functions contributing to TOE Security Functions shall be enabled by default.

P.Info_Flow: Flow of Information

The flow of information between IT components in a distributed architecture utilising insecure networks must be controlled and protected from disclosure.

P.Need_to_Know: User Need to Know

The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized Manager users which have a "need to know" for that information.

P.Notify: Notification of Failure

The TOE and the TSF will be capable of alerting and providing alarms in the event of a component, firmware, hardware or software failure.

4. SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

O.Access_Control: Access Control Policy

The TOE must uniquely identify and authenticate the claimed identity of Manager user and Subscriber user for Self-affiliation Facility, before granting a user access to TOE facilities. The access is based on Access Control Policy.

O.Alarm: Alarm Notification for Security Risks

The TOE will be capable of detecting a failure or error with any component, hardware, software, or firmware. The TOE will provide alarm capabilities for notification of security related events and of a failure or error.

O.Audit_Generation: Audit Records Generation

The TOE will provide the capability to detect and create readable records of security relevant events associated with Manager and Subscriber users.

O.Audit_Protection: Protect Audit Information

The TOE must provide the capability to protect audit information associated with individual Manager and Subscriber users.

O.Audit_Review: Review of Audit Records

The TOE will provide the capability to review audit information.

O.Correct_Routing: Correct Routing of Traffic

The TOE will correctly route traffic according to the switching parameters specified at connection set-up time in order to keep all the Subscriber's data separated from other Subscriber's data

O.Domain_Separation: Separation of Subscriber and Management Data Flow

The TOE must ensure the separation of Subscriber and Management Data flow

O.Fail_Secure: Preservation of Secure State for Failures

The TOE will preserve the secure state of the system in the event of a component or power failure.

O.Info_Flow: Information Flow Control

The TOE must ensure that Information Flow Control Policy is enforced.

O.Trusted_Recovery: Recovery Security State

Ensure the recovery to a secure state, without security compromise, after a discontinuity of operations. Ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the network.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.AFFILIATION

Those responsible for the operation of the TOE must ensure that Self-affiliating Subscribers have been advised of the requirements to de-affiliate from the present MPS, prior to attempting to affiliate at different one

OE.NETWORK_FRAGMENT

Those responsible for the operation of the TOE must ensure that a well-defined policy will be defined in order to avoid multiple presence of the same Subscriber user in the network as a consequence of later coalescence of fragments to the connected network

OE.POWER_SUPPLY

Those responsible for the operation of the TOE must ensure that MPS is provided with both external battery and mains power-supply when TOE is installed in a network

OE.RELIABLE_TIME_STAMP

Those responsible for the operation of the TOE must ensure that a well-defined policy will be defined and used for all the nodes in MPS network be synchronized with the same date and time.

OE.SECURE_ENVIRONMENT

Those responsible for the operation of the TOE must ensure that all the necessary environmental measures will be taken during network design, equipment installation and network deployment in order to assure data authentication and data confidentiality for Subscriber user data (e.g. by providing the presence of crypto equipment between TOE interfaces).

OE.TRUSTED_GATEWAY

Those responsible for the operation of the TOE must ensure that all the necessary physical and procedural security measures will be taken during network design, equipment installation and network deployment in order to assure that only trusted and non-hostile traffic is received at a Gateway Interface both from a Secure Capable Entity and Secure Uncapable Entity defined outside of the TOE security boundary

OE.TRAINING

Those responsible for the TOE must ensure that all personnel given administrator privileges are given training sufficient to enable them to fulfil their duties securely.

OE.TRUST

Those responsible for the TOE must ensure that only highly trusted Manager users are given privileges that enable them to modify the security configurations of the TOE.

5. IT SECURITY REQUIREMENTS

5.1 MANAGEMENT DATA

The following table depicts Management Data: both Security Attributes and TSF Data are reported with a characterization in terms of Permanent Data, Accounting Data and utilization in Access Control SFP and Information Flow Control SFP.

Changes to Management Data may result from explicit action by authorized Manager or by any other TSF-mediated actions under the control of Access Control SFP: data items that can be changed only by authorized Manager are indicated in *italic*; AC SFP and IFC SFP respectively indicate the fact that Access Control Policy and Information Flow Control Policy make use of Security Attributes or TSF Data specified:

Security Attributes	**Permanent Data**	**Accounting Data**	**AC SFP**	**IFC SFP**
Security Level of Trunk Interface	✓		✓	✓
Security Level of Access Interface	✓		✓	✓
Security Level of Gateway Interface	✓		✓	✓
Security Level of Subscriber	✓		✓	✓
Subscriber Capability of being downgraded	✓		✓	✓
Subscriber Capability for Self-affiliation Facility	✓		✓	
Subscriber status for Self-affiliation Facility			✓	
Security Level of Gateway	✓		✓	✓
Gateway Capability of being downgraded	✓		✓	✓
Gateway Interface Security Differentiator	✓		✓	✓
Security Level of PVC Connection	✓		✓	✓
PVC Connection Capability of being downgraded	✓		✓	✓
Security Level of sPVC Connection	✓		✓	✓
sPVC Connection Capability of being downgraded	✓		✓	✓
Switched Connection status				✓
Subscriber Personnel Identification Number	✓	✓	✓	
Manager Role Password	✓	✓	✓	
TSF Data	**Permanent Data**	**Accounting Data**	**AC SFP**	**IFC SFP**
Audit data trail	✓		✓	
Date and Time	✓		✓	✓
Manager Role accounting status		✓	✓	
Subscriber Self-affiliation Facility accounting status		✓	✓	

Table 3: Management Data specification

5.2 MANAGER ROLE

In the following table Management Data are indicated in relation with the capabilities of Manager Roles of reading and writing the single item:

Security Attribute	**Operator**	**Manager**	**Global**	**Lockout Admin**
Security Level of Trunk Interface	R	R/W	R/W	-
Security Level of Access Interface	R	R/W	R/W	-
Security Level of Gateway Interface	R	R/W	R/W	-
Security Level of Subscriber	R	R/W	R/W	-
Subscriber Capability of being downgraded	R	R/W	R/W	-
Subscriber Capability for Self-affiliation Facility	R	R/W	R/W	-
Subscriber status for Self-affiliation Facility	R	R/W	R/W	-
Security Level of Gateway	R	R/W	R/W	-
Gateway Capability of being downgraded	R	R/W	R/W	-
Gateway Interface Security Differentiator	R	R/W	R/W	-
Security Level of PVC connection	R	R/W	R/W	-
PVC Connection Capability of being downgraded	R	R/W	R/W	-
Security Level of sPVC connection	R	R/W	R/W	-
sPVC Connection Capability of being downgraded	R	R/W	R/W	-
Switched Connection Status	R	R/W	R/W	-
Subscriber Personnel Identification Number	-	W	W	-
Manager Role password	W [2]	W [3]	W [4]	W [5]
TSF Data	**Operator**	**Manager**	**Global**	**Security**
Audit data trail	R	R/W	R/W	-
Date and Time	R	R/W	R/W	-
Manager Role accounting status	-	-	-	W
Subscriber Self-affiliation Facility accounting status	R	R/W	R/W	-

Table 4: Capabilities of Manager Role with respect to Management Data

[2] Operator Role is capable of writing only Operator Role Password

[3] Manager Role is capable of writing Operator and Manager Roles Password

[4] Global Role is capable of writing Operator, Manager and Global Roles Password

[5] Lockout Admin Role is capable of writing only Lockout Admin Role Password

5.3 ACCESS CONTROL SFP

Access Control SFP is related to the rules enforced by the TSF in order to mediate any access to Management Data.

TSF enforces Access Control SFP by providing authorization to Manager users for successful beginning of a management session if and only if a correct combination of Manager Role identity and corresponding Password is provided.

TSF is not able to associate and maintain Manager user profiles to Management Roles for general management purpose, i.e. the TOE only has four acceptable management roles (Operator, Manager, Global and Lockout Admin), which have differing levels of access to the TSF. There is no distinguishing between two individuals who both have access to, e.g. the manager role/password, except by their log in/out times and session ids.

Access Control SFP also addresses Subscriber Self-affiliation Facility: each Subscriber capable of self-affiliating is required to dial a PIN (minimum length of six digits) in order to access TOE switching facilities.

Access Control SFP enforces that a Subscriber can be affiliated only once at a time at a local TOE and uses Information Flow Control SFP capabilities in order to check that the same Subscriber is not already affiliated at any node among the connected nodes in the network.

As a consequence, the Subscriber Self-affiliation Facility will successfully complete only if the same Subscriber is neither locally nor remotely detected.

The Access Control SFP provides an accounting locking mechanism for Operator, Manager, Global Roles and self-affiliating Subscribers when a pre-configured number of failed authentication attempts is reached: the exception to this is for the Lockout Admin Role, which may be used for resetting Manager Role account status and re-enable Manager users to authentication capability.

Manager and Global Roles may be used instead for resetting the Subscriber user accounting status and re-enable the Subscriber user to authentication capability associated to Self-affiliation Facility.

5.4 INFORMATION FLOW CONTROL SFP

Information Flow Control SFP is related to the rules enforced by TSF in order to manage incoming and outgoing Subscriber user data flows and Gateway data flows resulting from the successfully application of a well-defined mapping rule, defined at the TOE security boundaries between traffic flows outside of the TOE security boundary, associated both to Secure Capable and Secure Uncapable Entity, and traffic flows inside the TOE security boundary .

The well-defined mapping rule is based on the Gateway Interface Security Differentiator and the security information extracted from incoming signalling flow when that Gateway Interface is connected to a Secure Capable Entity, while is based on the Security Level of Gateway and Gateway Capability of being downgraded when that Gateway Interface is connected to a Secure Uncapable Entity.

The term “user data” here indicates the entire Subscriber user generated traffic (both Subscriber traffic and signalling data flow) received from one input port and switched towards an output port accordingly to the switching rules established by the TSF at connection setup time.

The term also indicates the signaling data flow terminated at the TOE that are used by a Subscriber user or by a trusted remote node for communicating to the TSF the relevant parameters to be used in order to establish a switched connection.

The term “Gateway data” here indicates both the traffic and signaling flows inside the TOE security boundary as a result of the application of a well-defined mapping rule at Gateway associated to Gateway Interfaces of the TOE.

Moreover Information Flow Control SFP is related to the rules enforced by TSF in order to manage both incoming and outgoing traffic and signaling flows associated to PVC and sPVC Connections between (s-)PVC Capable Interfaces.

TSF enforces Information Flow Control SFP in order to find a Subscriber in a connected network at connection setup time and, in combination with Access Control Policy SFP for Subscriber authentication, in order to guarantee Subscriber Self-affiliation Facility.

An exception to this is when the Subscriber is already affiliated in a remote node, which is temporarily not reachable by the routing algorithm because of the presence of a network fragment not connected; in case of multiple presence of the same Subscriber detected in the connected network at connection setup time the earliest affiliated Subscriber user will be considered by routing algorithm.

The Security Level of the affiliated Subscriber and associated capability of being downgradeable must be compatible with the Security Level of Access Interface the Subscriber is going to be affiliated to.

The Security Level and the associated capability of being downgradeable of a Gateway must be compatible with the Security Level of the Gateway Interface the Gateway is going to be associated to.

The Security Level and the associated capability of being downgradeable of a PVC and sPVC Connection must be compatible with the Security Level of the (s-)PVC Capable Interfaces involved in the Connection.

TSF enforces Information Flow Control SFP by avoiding the importing of management data coming from the outside of the TSF except for those imported from the Management Interface and processed accordingly to the Access Control SFP. In order to obtain that, TSF inhibits the flowing of any management data coming from any traffic interfaces (e.g. Trunk Interface).

At the same time all the security relevant information received from Trunk Interface and maintained by the TSF for call processing or routing algorithm, are stored in volatile memory with a scope limited to the lifetime of the connection.

Information Flow Control SFP ensures the correct switching of traffic flow inside the TOE, avoiding the erroneous exchange of Subscriber user, Gateway, PVC and sPVC associated data from one connection to another and ensuring that the processing of incoming signaling data flow do not affect in any way the integrity of local Management Data, preventing them from modifications in a way not mediated by the TSF.

To enforce Information Flow Control SFP, TSF implements a Multi-Level Secure (“MLS”) switching system based on both signaling data flow and relevant Management Data.

MLS is implicitly defined by the following rules:

- Routing algorithm capability to find a route able to support the call at a level equal or greater than the Security Level required by the initiator of the call (the crossing of a path in the route at a higher Security Level of the initiator doesn’t affect the Security Level of the call)
- Routing algorithm capability to find a route at successively lower Security Level starting from the Security Level of the initiator of the call if no route can be found according to the rule above and if the initiator of the call is registered with the capability of being downgraded. In case of multiple alternatives, the choice of the route shall be made on the basis of other configurable routing parameters (the crossing of a path in the route at a lower Security Level of the initiator does affect the Security Level of the call)
- Source and Destination Subscriber capability to be provided with Non-Secure Warning Tone by local TOE: when a call is established with a Security Level lower than the initiator and/or the recipient of the call, the TSF will provide the downgraded Subscriber(s) with the Non-Secure Warning Tone Indication

- Capability of exporting a pre-configured suitable label as a display indication towards terminal equipment able to support it
- Capability of dynamically adjust the Security Level of a call in case of Add-Party and Remove-Party for multipoint connections
- Capability of dynamically recalculate the provisioning of NSW tone to Subscribers in case of dynamic change of the Security Level of a call
- Capability of permanently connecting two (s-)PVC Capable Interfaces at the same node or at different nodes in the connected network via a switched call
- Capability of the TSF to apply a well-defined mapping rule between the traffic associated both to Secure Capable and Secure Uncapable Entities and flowing across a Gateway Interface and the traffic inside the TOE security boundary

The following table depicts the MLS rules enforced by Information Flow Control SFP for Subscriber users.

HL indicates a generic Higher Security Level Subscriber (higher than LL), LL indicates a generic Lower Security Level Subscriber (lower than HL).

The symbol ☎ indicates the fact that connection has been successfully set-up: the Security Level of the call (indicated nearby) may result lower than the Security Level of Subscriber offering the call when degradation occurs in the route established.

The symbol 🔔 indicates the generation of Non-Secure Warning indication in case of degraded call (A indicates the caller, also referred as Source, and B also referred as Destination, indicates the called)

The symbol ✋ indicates the call cannot be established in any case.

The actual security level of the call is shown in the display indication.

	Called Side (B)					
Caller Side (A)	**HL ⇔** Subscriber	**HL ⇓** Subscriber		**LL ⇔** Subscriber	**LL ⇓** Subscriber	
HL ⇔ Subscriber	☎ = HL	☎ = HL		✋	✋	
HL ⇓ Subscriber	☎ = HL	☎ = HL	☎ < HL 🔔 (A, B)	☎ = LL 🔔 (A)	☎ = LL 🔔 (A)	☎ < LL 🔔 (A, B)
LL ⇔ Subscriber	✋	☎ = LL 🔔 (B)		☎ = LL	☎ = LL	
LL ⇓ Subscriber	✋	☎ = LL 🔔 (B)	☎ < LL 🔔 (A, B)	☎ = LL	☎ = LL	☎ < LL 🔔 (A, B)

Table 5: Rules enforced by IFCP SFP for MLS policy in case of Subscriber users

The following table depicts the MLS rules enforced by Information Flow Control SFP for Gateway when connected to a Secure Uncapable Entity.

HL indicates a generic Higher Security Level Gateway (higher than LL), LL indicates a generic Lower Security Level Gateway (lower than HL).

The symbol ☎ indicates the fact that the switched connection has been successfully set-up: the Security Level of the call (indicated nearby) may result lower than the Security Level of Gateway offering the call when degradation occurs in the Route established.

The symbol ✋ indicates the call cannot be established in any case.

The well-defined mapping rule is to be intended as already applied at the moment of the application ot the following rules inside the TOE security boundary

	Called Side (B)					
Caller Side (A)	**HL** ⇔ Gateway	**HL** ⇓ Gateway		**LL** ⇔ Gateway	**LL** ⇓ Gateway	
HL ⇔ Gateway	☎ = HL	☎ = HL		✋	✋	
HL ⇓ Gateway	☎ = HL	☎ = HL	☎ < HL	☎ = LL	☎ = LL	☎ < LL
LL ⇔ Gateway	✋	☎ = LL		☎ = LL	☎ = LL	
LL ⇓ Gateway	✋	☎ = LL	☎ < LL	☎ = LL	☎ = LL	☎ < LL

Table 6: Rules enforced by IFCP SFP for MLS policy for Gateways

The following table depicts the MLS rules enforced by Information Flow Control SFP for a Gateway when connected to a Secure Capable Entity.

Secure Capable Entity traffic conditions are classified as:

- ONLY-SECURE (indicated as SSEC) traffic
- SECURE traffic (indicated as SEC)
- UNSECURE traffic (indicated as USEC)

ONLY-SECURE traffic indicates that only secure traffic conditions are accepted and signalled from/to connected entity; SECURE traffic indicates preferably secure traffic conditions signalled form/to connected entity; UNSECURE traffic is always mapped into non-secure conditions for MLS (indicated as NS).

The well-defined mapping rule is based on Gateway Interface Security Differentiator (indicated as SD) at both side of the call, information elements extracted from incoming signalling flow and security attributes associated to Gateway and Gateway Interface at both side of the call.

HL indicates a generic Higher Security Level Gateway (higher than LL), LL indicates a generic Lower Security Level Gateway (lower than HL): both HL and LL Gateway are intended as associated to a Secure Capable Entity.

The symbol ☎ indicates the fact that connection has been successfully set-up by TSF; if the call succeedes, the indication of the type of traffic condition offered to the Secure Capable Entity is indicated as well.

The symbol ✋ indicates the call cannot be established in any case.

HL and LL are supposed to be, in this case, alway different from non-secure bottom level indicated as NS in the table below.

		Called Side							
		SD ≤ HL		SD ≤ LL		SD > HL		SD > LL	
Caller Side		HL ⇔	HL ⇓	LL ⇔	LL ⇓	HL ⇔	HL ⇓	LL ⇔	LL ⇓
SSEC SD = HL / LL	HL ⇔	(SSEC) ☎ = HL	(SSEC) ☎ = HL	✋	✋	✋	✋	✋	✋
	LL ⇔	✋	(SSEC) SD ≤ ☎ = LL	(SSEC) ☎ = LL	(SSEC) ☎ = LL	✋	✋	✋	✋
SEC SD = HL / LL	HL ⇓	(SEC) ☎ = HL	(SEC) SD ≤ ☎ ≤ HL (USEC) ☎ = NS	(SEC) ☎ = LL	(SEC) SD ≤ ☎ ≤ LL (USEC) ☎ = NS	✋	(USEC) ☎ = NS	✋	(USEC) ☎ = NS
	LL ⇓	✋	(SEC) SD ≤ ☎ ≤ LL (USEC) ☎ = NS	(SEC) ☎ = LL	(SEC) SD ≤ ☎ ≤ LL (USEC) ☎ = NS	✋	(USEC) ☎ = NS	✋	(USEC) ☎ = NS
USEC	NS	✋	(USEC) ☎ = NS	✋	(USEC) ☎ = NS	✋	(USEC) ☎ = NS	✋	(USEC) ☎ = NS

Table 7: Rules enforced by IFCP for well-defined mapping rule at Gateway

The security attribute of “Gateway Capability of being downgraded” plays a special role when the associated Gateway Interface is involved in Conference Facility, in that dynamic changes in conference security level occurred at the TOE (as a consequence of the processing of Add-Party and Remove-Party requests for multipoint connections) are not propagated by the TSF across the Gateway Interface; for this reason when a Gateway is connected to a Secure Capable Entity and Conference Facility is required, the “Gateway Capability of being downgraded” should not be set for security to be maintained.

The following table depicts the MLS rules enforced by Information Flow Control SFP for PVC and sPVC Connections.

HL indicates a generic Higher Security Level (s-)PVC Capable Interface (higher than LL), LL indicates a generic Lower Security Level (s-)PVC Capable Interface (lower than HL).

Two different cases are taken into consideration depending on the fact that the connection flow is to be considered downgreadable or not.

The symbol ☎ indicates the fact that connection has been successfully set-up by TSF: the Security Level of the connection may result lower than the Security Level of the Source PVC or sPVC when degradation occurs in the route established.

	Destination Side (B)			
	Connection ⇔		**Connection ⇓**	
Source Side (A)	**HL** Interface	**LL** Interface	**HL** Interface	**LL** Interface
HL Interface	☎ = HL	✋	☎ <= HL	☎ <= LL
LL Interface	✋	☎ = LL	☎ <= LL	☎ <= LL

Table 8: Rules enforced by IFCP SFP for MLS policy for PVC and sPVC Connections

5.5 FAILURE MANAGEMENT

At the start-up and during the normal operations TSF is able to detect security relevant failures that may affect the correct behavior of the TOE.

Two types of failures are detected and processed by the TSF: failures detected at card level (“Card Failure”) and failures detected at network level (“Network Failure”).

The following table details the security relevant failures detected by TSF and indicate when the failures are recognized and processed.

Failure	**Event Description**	**Notes**
Card Failure	Hardware Failure	Detected at start-up time
	Software Monitoring Failure	Detected during normal operations
	Data Integrity Failure	Detected at start-up time
	Executable Code Failure	Detected at start-up time
	Master/Slave Failure	Detected during normal operations
Network Failure	Protocol Failure	Detected during normal operations
	Link Failure	Detected during normal operations

Table 9: Security relevant failure

5.6 TOE SECURITY FUNCTIONAL REQUIREMENTS

Functional Class	**Functional Components**
FAU	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4

FDP	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1,FDP_ETC.2, FDP_UIT.1
FIA	FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2
FMT	FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1
FPT	FPT_AMT.1, FPT_FLS.1, FPT_RCV.2, FPT_SEP.1, FPT_STM.1, FPT_TST.1
FRU	FRU_FLT.1, FRU_PRS.2
FTP	FTP_ITC.1, FTP_TRP.1

Table 10: Summary of Functional Requirement

5.6.1 SECURITY AUDIT (FAU)

5.6.1.1 Audit data generation (FAU_GEN.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 not specified level of audit; and

c) Changes to Management Data as a result of explicit action from Manager or as a result of any other TSF-mediated actions, Card Failure, Network Failure, results of the start-up diagnostic tests, Subscriber switched calls, prevention of audit data loss events. FAU_GEN.1.1

Refinement*: The audit record of start-up and shutdown of the audit functions are not explicitly generated; after a successful start-up, the TOE automatically provides an audit record for all the relevant auditable events: the first audit record generated represents the evidence of the start-up of the audit functions.*

Refinement: *Only successfully switched calls events shall generate audit records*

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, 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, the TSF shall record at least the following information: for the Subscriber and Gatewayswitched calls, the Source and the Destination identification, the Security Level of the call and the duration of each successfully switched call FAU_GEN.1.2

5.6.1.2 User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event. FAU_GEN.2.1

Application Note: *in the case of Manager user the identity is the Role; for Subscriber user and Gateway the identity is the phone number; for PVC and sPVC Connections is the connection identifier.*

5.6.1.3 Audit review (FAU_SAR.1)

The TSF shall provide authorized management personnel with the capability to read all audit data from the audit records. FAU_SAR.1.1

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

Application Note: *the term "user" here is to be intended as Manager user*

5.6.1.4 Protected audit trail storage (FAU_STG.1)

The TSF shall protect the stored audit records from unauthorized deletion. FAU_STG.1.1

The TSF shall be able to prevent modifications to the audit records. FAU_STG.1.2

5.6.1.5 Prevention of audit data loss (FAU_STG.4)

The TSF shall overwrite the oldest stored audit records and alert the Manager if the audit trail is full. FAU_STG.4.1

Application Note*: in order to prevent audit data loss a warning audit record is generated if a pre-configured threshold on the audit trail is exceeded*

5.6.2 USER DATA PROTECTION (FDP)

5.6.2.1 Subset access control (FDP_ACC.1)

The TSF shall enforce the Access Control SFP on access to all Management Data. FDP_ACC.1.1

5.6.2.2 Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the Access Control SFP to objects based on identification and authentication security attributes. FDP_ACF.1.1

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) Access of Managers to Management Data shall be conditioned on successfully authentication based on Manager Roles identification and Password.

b) Access of self-affiliating Subscriber to local switching facilities shall be conditioned on successful authentication based on entry of the Subscriber PIN. FDP_ACF.1.2

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

a) Checking compatibility between security attributes of Subscriber and Access Interface

b) Avoiding multiple presence of the same Subscriber in affiliated status at the local TOE

c) Avoiding multiple presence of the same Subscriber in affiliated status in the connected network using Information Flow Control SFP FDP_ACF.1.3

The TSF shall explicitly deny access of subjects to objects based on the violation of the Access Control SFP. FDP_ACF.14

5.6.2.3 Subset information flow control (FDP_IFC.1)

The TSF shall enforce the Information Flow Control SFP on

a) Traffic user data received form a far-end IT entity (e.g. a voice or data terminal equipment in case of Access Interface, a remote TOE or another trusted IT product in the operational environment inside the security boundaries), by checking flow integrity and switching user traffic in accordance with connection parameters established at connection set-up time

b) Signaling data received from a far-end IT entity (e.g. a suitable voice or data terminal equipment in case of Access Interface, a remote TOE or another trusted IT product in the operational environment inside the security boundaries), by checking packet integrity, storing of relevant information in a non-permanent way with a scope limited to the duration of the connection, checking the presence of Destination Subscriber, Gateway or (s-)PVC Capable Interfaces at the local TOE and searching for the Destination Subscriber, Gateway or (s-)PVC Capable Interface in the connected network by using flood search algorithm FDP_IFC.1.1

5.6.2.4 Simple security attributes (FDP_IFF.1)

The TSF shall enforce the Information Flow Control SFP based on the following types of subject and information security attributes:

a) Security Level of Source and Destination Subscribers, Gateways and Security Level of PVC and sPVC Connections

b) Security Level of Access, Gateway and Trunk Interfaces and Gateway Interface Security Differentiator

c) Subscriber, Gateway, PVC and sPVC Connection capability to support Multi-Level Secure calls

d) Subscriber capability to be provided with Non-Secure Warning Tone FDP_IFF.1.1

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

a) The integrity of the signaling message content is maintained

b) The integrity of user data traffic flow is maintained

c) Gateway and Gateway Interface capability to be provided with a well-defined mapping rule between traffic flowing across a Gateway Interface, associated both to Secure Capable and Secure Uncapable Entity, and traffic flowing inside the TOE Security Boundary FDP_IFF.1.2

The TSF shall enforce the following additional Information Flow Control SFP rules: none. FDP_IFF.1.3

The TSF shall provide the following list of additional Information Flow Control SFP capabilities:

a) Switched call security relevant information shall be stored in a non-permanent way with a scope limited to the duration of the connection

b) Capability of detecting multiple presence of the same Subscriber in the connected network for Subscriber Self-affiliation Facility FDP_IFF.1.4

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

a) Capability of establishing a switched connection between Source and Destination Subscribers, Gateways and (s-)PVC Capable Interfaces across a route at a Security Level equal or greater than the Security Level required by the initiator of the call for Subscriber and Gateway or the Security Level of Connection for PVC and sPVC; and

b) If no route can be found at the previous conditions, the capability of finding a route at successively lower Security Level starting from the Security Level required by the initiator of the call

c) Capability of Source and Destination Subscribers to be provided with Non-Secure Warning tone and indication where appropriate

d) Capability of re-arranging the security relevant parameters in case of dynamic changes of the Security Level of the call [FDP_IFF.1.5]

The TSF shall explicitly deny an information flow based on the following rules: rules based on the Information Flow Control SFP.[FDP_IFF.1.6]

***Application Note**: during call set-up time the capability to provide Non-Secure Warning tone is not able to be checked, but it depends on the correct working of underlying machine.*

5.6.2.5 Import of user data without security attributes (FDP_ITC.1)

The TSF shall enforce the Information Flow Control SFP when importing user data, controlled under the SFP, from outside of the TSC. [FDP_ITC.1.1]

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

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

a) Traffic user data will be switched accordingly to established connection channel

b) Signalling data are terminated at TSF and controlled under Information Flow Control SFP

c) The only Management Data that will be processed by TSF are those imported from the Management Interface. [FDP_ITC.1.3]

***Application Note**: user is to be intended as Subscriber user, Gateway or (s-)PVC Capable Interface. User data are to be intended as normal incoming traffic flow or signaling data: these data do not contain user security attributes conditioning the importing of the data themselves.*

5.6.2.6 Export of user data with security attributes (FDP_ETC.2)

The TSF shall enforce the Information Flow Control SFP when exporting user data, controlled under the SFP(s), outside of the TSC. [FDP_ETC.2.1]

The TSF shall export the user data with the user data's associated security attributes. [FDP_ETC.2.2]

The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data. [FDP_ETC.2.3]

The TSF shall enforce the following rules when user data is exported from the TSC:

a) Security Level of Trunk Interface will be exported if current Security Level of incoming call is greater than the Security Level of the chosen trunk at connection set up time

b) A label providing a suitable display indication will be exported towards terminal equipment involved in a call [FDP_ETC.2.4]

***Application Note**: user is to be intended as Subscriber user, Gateway or (s-)PVC Capable Interface.*

5.6.2.7 Data exchange integrity (FDP_UIT.1)

The TSF shall enforce the Information Flow Control SFP to be able to transmit, receive user data in a manner protected from modification errors. [FDP_UIT.1.1]

The TSF shall be able to determine on receipt of user data, whether modification has occurred. [FDP_UIT.1.2]

***Application Note**: user is to be intended as Subscriber user; the TSF shall only be able to determine non-malicious modifications in user data*

5.6.3 IDENTIFICATION AND AUTHENTICATION (FIA)

5.6.3.1 Authentication failure handling (FIA_AFL.1)

The TSF shall detect when a pre-configured number of unsuccessful authentication attempts occur related to Management Data access and Subscriber authentication. [FIA_AFL.1.1]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prohibit access by the Manager or Subscriber to Management Data. The exception to this shall be the Lockout Admin manager role on the Management Interface. [FIA_AFL.1.2]

5.6.3.2 Verification of secrets (FIA_SOS.1)

The TSF shall provide a mechanism to verify that secrets meet a High Strength of Function. [FIA_SOS.1.1]

5.6.3.3 User authentication before any action (FIA_UAU.2)

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

***Application Note**: user is to be intended both as Manager and Subscriber user*

5.6.3.4 User identification before any action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. [FIA_UID.2.1]

***Application Note**: user is to be intended both as Manager and Subscriber user*

5.6.4 SECURITY MANAGEMENT (FMT)

5.6.4.1 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the Access Control SFP to restrict the ability to query the security attributes of all Management Data but “Subscriber Personnel Identification Number” and “Manager Role password” to “Operator”, “Manager” and “Global” Roles. [FMT_MSA.1.1A]

The TSF shall enforce the Access Control SFP to restrict the ability to change default, modify the security attributes of all Management Data but Accounting Data (see also FMT_MTD.1) to “Manager” and “Global” Manager Role. [FMT_MSA.1.1B.1]

The TSF shall enforce the Access Control SFP to restrict the ability to change default, modify the security attribute of “Manager Role password” associated to “Operator” Role to “Operator”, “Manager”and “Global” Manager Role. [FMT_MSA.1.1B.2]

The TSF shall enforce the Access Control SFP to restrict the ability to change default, modify the security attribute of "Manager Role password" associated to "Manager" Role to "Manager"and "Global" Manager Role. FMT_MSA.1.1B.3

The TSF shall enforce the Access Control SFP to restrict the ability to change default, modify the security attribute of "Manager Role password" associated to "Global" Manager Role to "Global" Manager Role. FMT_MSA.1.1B.4

The TSF shall enforce the Access Control SFP to restrict the ability to change default, modify the security attribute of "Manager Role password" associated to "Lockout Admin" Role to "Lockout Admin" Manager Role. FMT_MSA.1.1B.5

The TSF shall enforce the Access Control SFP to restrict the ability to modify and delete the security attributes of "Manager Role accounting status" to "Lockout Admin" Manager Role. FMT_MSA.1.1C

The TSF shall enforce the Access Control SFP to restrict the ability to modify the security attributes of "Subscriber Self-affiliation Facility accounting status" to "Manager" and "Global" Manager Role. FMT_MSA.1.1D

***Refinement**: "Manager Role accounting status" cannot be read by any Manager Role*

***Application Note**: Operator Role is capable of writing only Operator Role Password, Manager Role is capable of writing Operator and Manager Roles Password, Global Role is capable of writing Operator, Manager and Global Roles Password, Lockout Admin Role is capable of writing only Lockout Admin Manager Role Password; all Manager Roles are not capable of reading Manager Role Passwords and Subscriber Personal Identification Number*

5.6.4.2 Static attribute initialization (FMT_MSA.3)

The TSF shall enforce the Access Control SFP to provide restrictive default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

The TSF shall allow the authorized Manager Roles to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

***Application Note**: the TSF shall not allow any Manager Role to specify alternative values to override the factory default data.*

5.6.4.3 Management of TSF Data (FMT_MTD.1)

The TSF shall restrict the ability to clear Audit Data to "Manager", and "Global" Manager Roles. FMT_MTD.11A

The TSF shall restrict the ability to query Audit Data to "Operator", "Manager" and "Global" Manager Roles. FMT_MTD.11B

5.6.4.4 Security roles (FMT_SMR.1)

The TSF shall maintain the roles Operator, Manager, Global and Lockout Admin. FMT_SMR.1.1

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

***Application Note**: user is to be intended as Manager user; the TSF does not provide management of user profiles but only authorized users with their associated manager role as user identity*

5.6.5 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

5.6.5.1 Abstract machine testing (FPT_AMT.1)

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

***Application Note**: The text "abstract machine that underlies the TSF" must be interpreted as a permanent diagnostic process providing software monitoring of all the parts of the TOE related to security relevant aspects*

5.6.5.2 Failure with preservation of secure state (FPT_FLS.1)

The TSF shall preserve a secure state when the following types of failures occur: Card Failure and Network Failure. [FPT_FLS.1.1]

***Application Note**: In case of power failure when supplied with mains, the TOE must be provided with external battery power supply: the TOE suppports automatic changeover*

5.6.5.3 Automated recovery (FPT_RCV.2)

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. [FPT_RCV.2.1]

For Card Failure the TSF shall ensure the return of the TOE to a secure state using automated procedures. [FPT_RCV.2.2]

***Application Note**: The term "Automatic Recovery" must be interpreted as an automatic switchover of Management and Control Plane for MPS115 when equipped in redundant configuration*

5.6.5.4 TSF domain separation (FPT_SEP.1)

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

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

5.6.5.5 Reliable time stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. [FPT_STM.1.1]

***Application Note**: the responsibility of setting and maintain a correct date and time is outside the scope of TSF; the TSF does simply guarantee a reliable real-time clock source*

5.6.5.6 TSF testing (FPT_TST.1)

The TSF shall run a suite of self-tests during initial start-up and periodically during normal operation to demonstrate the correct operation of the TSF.[FPT_TST.1.1]

The TSF shall provide authorized users with the capability to verify the integrity of TSF data. [FPT_TST.1.2]

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. [FPT_TST.1.3]

***Application Note**: user is to be intended as Manager user; failures in data and executable code integrity are reported as Card Failure conditions*

5.6.6 RESOURCE UTILIZATION (FRU)

5.6.6.1 Degraded fault tolerance (FRU_FLT.1)

The TSF shall ensure the operation of maintaining all security functionalities except the ones performed by the entities involved when the following failures occur: Card failure and Network failure. FRU_FLT.1.1

5.6.6.2 Full priority of service (FRU_PRS.2)

The TSF shall assign a priority to each subject in the TSF. FRU_PRS.2.1

The TSF shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects' assigned priority. FRU_PRS.2.2

5.6.7 TRUSTED PATH/CHANNELS (FTP)

5.6.7.1 Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. FTP_ITC.1.1

The TSF shall permit the TSF and the remote trusted IT product to initiate communication via the trusted channel. FTP_ITC.1.2

The TSF shall initiate communication via the trusted channel for the transmission of control information and transfer of security attributes. FTP_ITC.1.3

***Refinement**: FTP_ITC.1.1 states that "and protection of the channel data from modification". For the purpose of this Security Target, protecting channel data from modification and disclosure is optional for the implementation of this requirement.*

***Application Note:** The remote trusted IT product refers to another network system or IT product. A Trusted Channel provides a means for clients to perform functions through an assured connection at some level from TOE to other network systems or IT product. A trusted channel is used to transmit control information. The control information consists of messages exchanged across the signaling channel or hardware control signal transmitted from the TOE to remote devices.*

5.6.7.2 Trusted path (FTP_TRP.1)

The TSF shall provide a communication path between itself and local Manager and Subscriber users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. FTP_TRP.1.1

The TSF shall permit local Manager and Subscriber user to initiate communication via the trusted path. FTP_TRP.1.2

The TSF shall require the use of the trusted path for initial user authentication transmission of network management information and initial Subscriber user authentication for Self-affiliation Facility. FTP_TRP.1.3

***Refinement**: FTP_TRP.1.1 states that "and protection of the communicated data from modification". For the purpose of this ST, protecting communicated data from modification and disclosure is optional for the implementation of this requirement. This requirement has been refined for FTP_TRP.1.1 and FTP_TRP.1.2 to include all authorized local Manager Roles and Subscriber Users. All authorized local Manager Roles and authorized Subscriber user capable of Self-affiliation Facility shall be permitted to initiate communication via the trusted path.*

***Application Note**: a Trusted Path is a communication path for which exchanges may be initiated by either side of the channel and both ends of the path are identifiable. A trusted path contains identified subsets of TSF data and commands. For the purpose of this ST a trusted path is the network management link or the Access Interface link. Therefore, one end of the path is the network management station or the access telephone device and the other end is the TOE that is being managed or accessed.*

5.7 STRENGTH OF FUNCTION CLAIM

An overall strength of function claim of SOF-high is made for the TOE.

5.8 TOE SECURITY ASSURANCE REQUIREMENTS

Assurance Class	**Assurance Components**
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.2 AVA_SOF.1 AVA_VLA.2
Assurance Class	**Augmenting Components**
ALC	ALC_FLR.1

Table 11: Summary of Assurance Requirements (EAL4 +)

5.8.1 CONFIGURATION MANAGEMENT (ACM)

5.8.1.1 Partial CM automation (ACM_AUT.1)

The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation. ACM_AUT.1.1C

The developer shall use a CM system. ACM_AUT.1.1D

The CM system shall provide an automated means to support the generation of the TOE. ACM_AUT.1.2C

The developer shall provide a CM plan. ACM_AUT.1.2D

The CM plan shall describe the automated tools used in the CM system. ACM_AUT.1.3C

The CM plan shall describe how the automated tools are used in the CM system. ACM_AUT.1.4C

5.8.1.2 Generation support and acceptance procedures (ACM_CAP.4)

The CM system shall provide measures such that only authorized changes are made to the configuration items. ACM_CAP.4.10C

The CM system shall support the generation of the TOE. ACM_CAP.4.11C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE. ACM_CAP.4.12C

The reference for the TOE shall be unique to each version of the TOE. ACM_CAP.4.1C

The developer shall provide a reference for the TOE. ACM_CAP.4.1D

The TOE shall be labeled with its reference. ACM_CAP.4.2C

The developer shall use a CM system. ACM_CAP.4.2D

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan. ACM_CAP.4.3C

The developer shall provide CM documentation. ACM_CAP.4.3D

The configuration list shall describe the configuration items that comprise the TOE. ACM_CAP.4.4C

The CM documentation shall describe the method used to uniquely identify the configuration items. ACM_CAP.4.5C

The CM system shall uniquely identify all configuration items. ACM_CAP.4.6C

The CM plan shall describe how the CM system is used. ACM_CAP.4.7C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan. ACM_CAP.4.8C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system. ACM_CAP.4.9C

5.8.1.3 Problem tracking CM coverage (ACM_SCP.2)

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws. ACM_SCP.2.1C

The developer shall provide CM documentation. ACM_SCP.2.1D

The CM documentation shall describe how configuration items are tracked by the CM system. ACM_SCP.2.2C

5.8.2 DELIVERY AND OPERATION (ADO)

5.8.2.1 Detection of modification (ADO_DEL.2)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site. ADO_DEL.2.1C

The developer shall document procedures for delivery of the TOE or parts of it to the user. ADO_DEL.2.1D

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site. ADO_DEL.2.2C

The developer shall use the delivery procedures. ADO_DEL.2.2D

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site. ADO_DEL.2.3C

5.8.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. ADO_IGS.1.1C

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. ADO_IGS.1.1D

5.8.3 DEVELOPMENT (ADV)

5.8.3.1 Fully defined external interfaces (ADV_FSP.2)

The functional specification shall describe the TSF and its external interfaces using an informal style. ADV_FSP.2.1C

The developer shall provide a functional specification. ADV_FSP.2.1D

The functional specification shall be internally consistent. ADV_FSP.2.2C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages. ADV_FSP.2.3C

The functional specification shall completely represent the TSF. ADV_FSP.2.4C

The functional specification shall include rationale that the TSF is completely represented. ADV_FSP.2.5C

5.8.3.2 Security enforcing high-level design (ADV_HLD.2)

The presentation of the high-level design shall be informal. ADV_HLD.2.1C

The developer shall provide the high-level design of the TSF. ADV_HLD.2.1D

The high-level design shall be internally consistent. ADV_HLD.2.2C

The high-level design shall describe the structure of the TSF in terms of subsystems. ADV_HLD.2.3C

The high-level design shall describe the security functionality provided by each subsystem of the TSF. ADV_HLD.2.4C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. ADV_HLD.2.5C

The high-level design shall identify all interfaces to the subsystems of the TSF. ADV_HLD.2.6C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. ADV_HLD.2.7C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate. ADV_HLD.2.8C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. ADV_HLD.2.9C

5.8.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions. ADV_IMP.1.1C

The developer shall provide the implementation representation for a selected subset of the TSF. ADV_IMP.1.1D

The implementation representation shall be internally consistent. ADV_IMP.1.2C

5.8.3.4 Descriptive low-level design (ADV_LLD.1)

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules. ADV_LLD.1.10C

The presentation of the low-level design shall be informal. ADV_LLD.1.1C

The developer shall provide the low-level design of the TSF. ADV_LLD.1.1D

The low-level design shall be internally consistent. ADV_LLD.1.2C

The low-level design shall describe the TSF in terms of modules. ADV_LLD.1.3C

The low-level design shall describe the purpose of each module. ADV_LLD.1.4C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules. ADV_LLD.1.5C

The low-level design shall describe how each TSP-enforcing function is provided. ADV_LLD.1.6C

The low-level design shall identify all interfaces to the modules of the TSF. ADV_LLD.1.7C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible. ADV_LLD.1.8C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate. ADV_LLD.1.9C

5.8.3.5 Informal correspondence demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. ADV_RCR.1.1C

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. ADV_RCR.1.1D

5.8.3.6 Informal TOE security policy model (ADV_SPM.1)

The TSP model shall be informal. ADV_SPM.1.1C

The developer shall provide a TSP model. ADV_SPM.1.1D

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled. ADV_SPM.1.2C

The developer shall demonstrate correspondence between the functional specification and the TSP model. ADV_SPM.1.2D

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled. ADV_SPM.1.3C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. ADV_SPM.1.4C

5.8.4 GUIDANCE DOCUMENTS (AGD)

5.8.4.1 Administrator guidance (AGD_ADM.1)

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE. AGD_ADM.1.1C

The developer shall provide administrator guidance addressed to system administrative personnel. AGD_ADM.1.1D

The administrator guidance shall describe how to administer the TOE in a secure manner. AGD_ADM.1.2C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. AGD_ADM.1.3C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE. AGD_ADM.1.4C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. AGD_ADM.1.5C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. AGD_ADM.1.6C

The administrator guidance shall be consistent with all other documentation supplied for evaluation. AGD_ADM.1.7C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. AGD_ADM.1.8C

5.8.4.2 User guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. AGD_USR.1.1C

The developer shall provide user guidance. AGD_USR.1.1D

The user guidance shall describe the use of user-accessible security functions provided by the TOE. AGD_USR.1.2C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. AGD_USR.1.3C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment. AGD_USR.1.4C

The user guidance shall be consistent with all other documentation supplied for evaluation. AGD_USR.1.5C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user. AGD_USR.1.6C

5.8.5 LIFE CYCLE SUPPORT (ALC)

5.8.5.1 Identification of security measures (ALC_DVS.1)

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.1.1C

The developer shall produce development security documentation. ALC_DVS.1.1D

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.1.2C

5.8.5.2 Developer defined life-cycle model (ALC_LCD.1)

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE. ALC_LCD.1.1C

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE. ALC_LCD.1.1D

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE. ALC_LCD.1.2C

The developer shall provide life-cycle definition documentation. ALC_LCD.1.2D

5.8.5.3 Well-defined development tools (ALC_TAT.1)

All development tools used for implementation shall be well defined. ALC_TAT.1.1C

The developer shall identify the development tools being used for the TOE. ALC_TAT.1.1D

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation. ALC_TAT.1.2C

The developer shall document the selected implementation-dependent options of the development tools. ALC_TAT.1.2D

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options. ALC_TAT.1.3C

5.8.6 TESTS (ATE)

5.8.6.1 Analysis of coverage (ATE_COV.2)

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. ATE_COV.2.1C

The developer shall provide an analysis of the test coverage. ATE_COV.2.1D
The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. ATE_COV.2.2C

5.8.6.2 Testing: high-level design (ATE_DPT.1)

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design. ATE_DPT.1.1C

The developer shall provide the analysis of the depth of testing. ATE_DPT.1.1D

5.8.6.3 Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. ATE_FUN.1.1C

The developer shall test the TSF and document the results. ATE_FUN.1.1D

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed. ATE_FUN.1.2C

The developer shall provide test documentation. ATE_FUN.1.2D

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests. ATE_FUN.1.4C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. ATE_FUN.1.5C

5.8.6.4 Independent testing - sample (ATE_IND.2)

The TOE shall be suitable for testing. ATE_IND.2.1C

The developer shall provide the TOE for testing. ATE_IND.2.1D

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ATE_IND.2.2C

5.8.7 VULNERABILITY ASSESSMENT (AVA)

5.8.7.1 Validation of analysis (AVA_MSU.2)

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation. AVA_MSU.2.1C

The developer shall provide guidance documentation. AVA_MSU.2.1D

The guidance documentation shall be complete, clear, consistent and reasonable. AVA_MSU.2.2C

The developer shall document an analysis of the guidance documentation. AVA_MSU.2.2D

The guidance documentation shall list all assumptions about the intended environment. AVA_MSU.2.3C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls). AVA_MSU.2.4C

The analysis documentation shall demonstrate that the guidance documentation is complete. AVA_MSU.2.5C

5.8.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

For each mechanism with strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST. AVA_SOF.1.1C

The developer shall perform strength of TOE security function analysis for each mechanism identified in the ST as having strength of TOE security function claim. AVA_SOF.1.1D

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST. AVA_SOF.1.2C

5.8.7.3 Independent vulnerability analysis (AVA_VLA.2)

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. AVA_VLA.2.1C

The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP. AVA_VLA.2.1D

The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks. AVA_VLA.2.2C

The developer shall document the disposition of identified vulnerabilities. AVA_VLA.2.2D

5.8.7.4 Basic Flaw Remediation (ALC_FLR.1)

The developer shall document the flaw remediation procedures. ALC_FLR.1.1D

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE. ALC_FLR.1.1C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.1.2C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. ALC_FLR.1.3C

The flaw remediation procedures documentation shall describe the method used to provide flaw information, corrections and guidance on corrective actions to TOE users. ALC_FLR.1.4C

6. TOE SUMMARY SPECIFICATIONS

This section presents the Security Functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that the TOE must satisfy.

6.1 IT SECURITY FUNCTION

The IT Security Functions are organized in functional groups that cover all the TOE-specific elaboration of the Security Functional Requirements the TOE has supported.

IT security functions covers all Security Functional Requirements and each IT Security Function is mapped onto at least one Security Functional Requirement.

This section is written primarily for evaluators and consumers.

The functional Security Function groups are as follows:

- Identification and Authorization
- User Data Protection
- Auditing
- Intrusion Detection
- Protection and Recovery

6.1.1 IDENTIFICATION AND AUTHORIZATION SECURITY FUNCTIONS

It identifies the following Security Functions:

SF	SFR	Description
User Identification	FIA_UID.2	User Identification before any action
User Authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User authentication before any action
	FTP_TRP.1	Trusted Path

User Identification

The TOE provides an asynchronous serial port supporting an interactive facility controller interface that can be used for management purposes: using a video display unit or a basic terminal emulator, users can logon, start a local management session and access security-relevant information maintained by the TOE.

At the same time the TOE provides an Ethernet port supporting a data exchange interface based on a proprietary, message-oriented binary protocol that can be used for remote, out-of-band, management purposes: using the proprietary protocol, users can start a remote management session and access security-relevant information maintained by the TOE.

Users at the local management port are prompted with a login request and they must supply a “Manager Role” in order to start a local management session.

Users at the remote management port are requested for a “Manager Role” in the login message in order to start a remote management session.

A user is not allowed by the implementation to perform any action before being identified (FIA_UID.2).

User Authentication

Users at the local management port are prompted with a login request and they must supply a “Password” in order to start a local management session (FTP_TRP.1).

Users at the remote management port are requested for a “Password” in the login message in order to start a remote management session (FTP_TRP.1).

The TOE provides Self-affiliation Facility, by which a registered subscriber, after network deployment can move inside the network and use different nodes, self-affiliating by means of a voice (or data) terminal equipment, provides, as a side-effect, the modification of security-relevant information maintained by the TOE.

The self-affiliated condition for a Subscriber user is not permanent and is not mainatained by the TOE after a power-off o reset event occurred at the TOE.

Subscribers connected at local voice or data terminal equipment must dial a “Personal Identification Number” in order to affiliate at the local switch and access the circuit switch facilities (FTP_TRP.1).

Both data management and subscriber users are not allowed by the implementation to perform any action before being authenticated (FIA_UAU.2).

High Strength of Function is met by the secret (the “Password”) for the management session: at least eight characters must be supplied and case-sensitive check is enforced (FIA_SOS.1).

High Strength of Function is met by PIN for Subscriber user self-affiliation facility: at least six digits must be entered (FIA_SOS.1).

Should the authentication algorithm fail for a pre-configured number of times, the user account associated at that Manager Role would automatically be locked (FIA_AFL.1).

6.1.2 USER DATA PROTECTION SECURITY FUNCTIONS

It identifies the following Security Functions:

SF	SFR	Description
Local Management Port Access	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security attribute based access control
	FMT_SMR.1	Security Roles
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
Remote Management Port Access	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security attribute based access control

	FMT_SMR.1	Security Roles
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
Local Subscriber Affiliation	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security attribute based access control
	FMT_MSA.3	Static Attribute Initialization
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
User Accounting	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SMR.1	Security Roles
Information Flow Control	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ETC.2	Export of user data with security attribute
	FMT_MSA.3	Static Attribute Initialization
	FDP_UIT.1	Data exchange integrity

Local Management Port Access

The local management port access control Security Function enforces the policy for accessing all the user configuration data (FDP_ACC.1).

The pair “Manager Role” and “Manager Role Password”, provided by the user during identification and authorization, will be used for user authentication and allows authorized user to logon and start a local management session at the local management port (FDP_ACF.1).

The implementation provides local management port access control by defining user roles with different capabilities with respect to Management Data (FMT_MSA.1); at each role is assigned a Manager Role and Password, and the implementation is able to associate authorized users with roles by matching Manager Role identifier and Password derived from the identification and authentication phase (FMT_SMR.1).

The TOE for accessing the TSF provides the following roles:

- Operator Role
- Manager Role
- Global Role
- Lockout Admin Role

The TOE, as a default, statically assigns access rights for any newly created objects to Manager users accordingly to their associated Manager Role (FMT_MSA.3).

Remote Management Port Access

The proprietary protocol implements the same control access rules based on Manager Role and Manager Role Password associating roles to user in the same way already specified for the local management port access control Security Function.

Local Subscriber Affiliation

The local subscriber affiliation access control Security Function, enforces the policy for accessing the user configuration data (FDP_ACC.1).

Using the voice or data terminal equipment the user is requested to dial the affiliation facility code and a Personal Identification Number associated with its profile; the correct PIN verification allows user to access the circuit switch facilities (FDP_ACF.1).

The SF checks for the presence of the same user as affiliated user in the local node (FDP_ACF.1).

Each time a user becomes registered in the switch the default configuration disables the access to switching facilities (FMT_MSA.3) and the user becomes a potential Subscriber: in order to access switching facilities, Subscriber must be aware that he has to dial his PIN, if he has been profiled as capable of Self-Affiliation or has to expect an explicit Manager action.

Self-affiliation procedure implements both a check of compatibility between security features of the Subscriber user against Access Interface the Subscriber user requests to be affiliated to (FDP_IFF.1) and a check of multiple presence of the same Subscriber user in the connected network (FDP_IFC.1).

In case of multiple presence of the same Subscriber user detected in the network at call setup time as a consequence of the coalescence of a network fragment previously isolated to the connected network, the earliest affiliated Subscriber user will be considered.

User Accounting

The User Authentication SF specified above, provides an accounting locking mechanism for Manager users and self-affiliating Subscriber users when a pre-configured number of failed authentication attempts is reached; TOE implementation fixes at three the maximum number of attempts for successfully authentication process both for Manager and Subscriber user before account locking mechanism took over; after account locking, in order to restore the normal operations in term of TOE usage from the Management Interfaces and from the Access Interface for Self-affilition capable Subscriber user, an unlocking mechanism is provided by User Accounting SF as well; a restriction on unlocking of accounts is implemented for the “Lockout Admin” Manager Role (FMT_MSA.3), which is the only Manager Role authorized to reset accounting status and re-enable Manager users to authentication facility (FMT_MSA.1); a restriction on unlocking of accounts is implemented for the “Manager” and “Global” Manager Role (FMT_MSA.3), which are the only Manager Roles authorized to reset accounting status and re-enable Subscriber users to the normal operations at Access Interfaces.

Only “Operator”, “Manager” and “Global” Manager Roles among those defined for the TOE (FMT_SMR.1) are subject to locking mechanism of Manager user account.

Information Flow Control

When a caller subscriber requests access to the local node switching facilities a call setup message is generated or processed by the switch in order to locate the called subscriber in the local switch or the network and serve the request.

The call control information flow control Security Function enforces the policy for accessing the local switching facilities and reserve bandwidth to the user (FDP_IFC.1).

In order to guarantee the Multi Level Secure Circuit Switched calls policy, the choice of processing and forwarding the subscriber request or not is conditioned by the security level of underlying infrastructure, the matching between the security level attribute of the initiator and recipient of the call and

the capability of source and destination to be provided with the generation of Non-Secure-Warning tone in case of the degradation of the security level of the connection, where appropriate (FDP_IFF.1).

The initiator and recipient of the call are to be considered as authorized Subscriber Users at Access Interfaces, Gateways at Gateway Interfaces or (s-)PVC Capable Interfaces in the same node or in different nodes across the network and inside the TOE security boundary (FDP_IFF.1)

Factory default configuration data from which user profiles are derived are intrinsically secure (FMT_MSA.3).

The call processing implementation doesn't affect in any way the nature of the user data transmitted or received during the signaling and/or routing process (FDP_UIT.1).

During call establishment phase, the TSF is able to terminate signalling data flow carried by signalling communication channel and import security relevant parameters used by TSF itself in order to process the incoming call (FDP_ITC.1).

When processing an incoming call setup request, the TSF is able to select a convenient output path in accordance with the Security Level of the call and the downgradeable feature of Source Subscriber and exporting either the Security Level of Trunk Interface stored as a Management Data in case of forwarding the call to the connected network, or exporting a suitable display indication, where appropriate, in case of local connection to Destination Subscriber (FDP_ETC.2).

6.1.3 AUDITING SECURITY FUNCTION

The following Security Functions are identified:

SF	SFR	Description
Audit Data Generation	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FPT_STM.1	Reliable time stamps
	FMT_MSA.3	Static Attribute Initialization
Audit Data management	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
	FMT_SMR.1	Security Roles
	FMT_MTD.1	Management of TSF data

Audit Data Generation SF

The implementation continuously monitors, keeps trace and updates the operational state of all the critical components of the equipment.

An event logging facility is available in order to generate audit record (FAU_GEN.1).

The facility is based on the availability of a local reliable time source, which is able to produce date-time information used for reliable time stamps associated at each audit record (FPT_STM.1).

As a default, the TOE provides the Audit data records for all the security relevant events, without any Manager user intervention (FMT_MSA.3).As far as the security aspects are concerned, an audit record is generated for the following security-relevant events and activities:

- Changing of relevant security attributes
- Teardown of switched connections
- Card unit failure
- Link failure
- Protocol failure
- Log queue critical threshold reached
- Log queue overflow

Changing of relevant security attributes audit record contains date and time, the outcome of the event and all the relevant information for the correct interpretation of the date change depending on the context in which the changes has been made (FAU_GEN.1).

Teardown of switched connections audit record contains date and time of the event, the indication of setup or teardown, the outcome (success or failure) of the event (FAU_GEN.1), the Source and Destination address relevant information, the Security Level of the call and the duration of the call (FAU_GEN.2).

Card and link failure audit record contains date and time of the event, the indication of the type of fault or failure (FAU_GEN.1) and the indication of the card or link associated with the fault (FAU_GEN.2).

Log queue critical threshold reached and over flow audit record are associated with the logging policy and contains date and time of the events, the indication of the type of event, the outcome of the operation (FAU_GEN.1) and the indication of the threshold reached or the indication of overflow respectively (FAU_GEN.2).

Audit Data Management

All the information generated as a consequence of security relevant events detected by the implementation and organized as audit records are stored in a internal, battery-powered backup memory; the information is available for retrieval and presented in a suitable manner in order to ease audit analysis (FAU_SAR.1).

The collected and stored audit information is only available at authorized users that have successfully initiated a management session (FAU_SAR.1).

The implementation organizes audit record in a fixed-size circular buffer and the relevant events are queued in the same order as they occur; when the number of the stored audit records exceeds the size of the buffer, the oldest stored audit record is overwritten (FAU_STG.1).

The first new stored audit record, will be an alert to the local manager that the oldest record has been overwritten using the log queue overflow event indication; moreover an event of log queue critical threshold reached will be raised in the case of a critical threshold is reached in the number of current audit record stored in the queue buffer. This will provide the local manager with an alert that a retrieval of the currently stored audit record should be made in order to avoid the loss of information (FAU_STG.4).

The TOE prevents unauthorized users from modifying or deleting of audit records (FAU_STG.1).

Only authorized user with associated the Manager, Global Role are able to reset the content of the buffer (FMT_MTD.1and FMT_SMR.1).

6.1.4 INTRUSION DETECTION SECURITY FUNCTION

It identifies the following Security Functions:

SF	SFR	Description
Domain Separation	FPT_SEP.1	TSF Domain Separation
	FDP_ITC.1	Import of user data without security attributes
	FDP_IFC.1	Subset information flow control
	FTP_ITC.1	Inter-TSF trusted channel

Domain Separation SF

The TSF shall maintain, during normal operations, a security domain for its own execution that protects it from interference and tampering by untrusted subjects and enforce separation between the security domains of subjects in the TSC (FPT_SEP.1).

The management plane implementation does not process any management data from any interface except for the dedicated management interface according to the local management port and remote management port SFP (FDP_ITC.1).

In any case user data integrity won't be lost as an effect of call processing elaboration or as an effect of allocating switching resources to different users (FDP_ITC.1).

Domain Separation applies both to traffic user data and to signalling data (FDP_IFC.1).

TSF is able to setup a communication channel between a far-end IT entity and the local TOE in order to transmit and receive singalling data (FTP_ITC.1).

6.1.5 PROTECTION AND RECOVERY SECURITY FUNCTION

It identifies the following Security Functions:

SF	SFR	Description
Testing	FPT_AMT.1	Abstract machine testing
	FPT_TST.1	TSF testing
Failure Management	FPT_FLS.1	Failure with preservation of secure state
Protection	FPT_RCV.2	Automated recovery
	FRU_FLT.1	Degraded fault tolerance
	FRU_PRS.2	Full priority of service

Testing

The equipment has been designed for local and remote troubleshooting by including self-test circuits and procedure to make location and confinement of the malfunction on the replaceable units easier.

The test sequences are activated automatically at the equipment power-on during the startup process (FPT_AMT.1); the status of the system is continuously tested by software monitoring processes in order to prevent and detect possible deviations from the correct operations of the single component of the system implementation (FPT_TST.1).

Failure Management

During the normal operation the following failure conditions are automatically detected by the implementation:

- Card failure
- Network failure

Each single failure doesn't affect the correct operation of other parts of the system and preservation of the normal operations has been obtained by isolating the single failure (FPT_FLS.1).

Protection

In case of recognized card or network failure the implementation is able to restore the previous configuration in order to bring the equipment to a secure state (FRU_FLT.1).

In particular, in case of Network Failure, the TSF will be able to drive hardware trusted channel in order to transmit control signal information related to the synchronization of a remote IT trusted product (FTP_ITC.1).

The hardware trusted channel will be used for driving electrical impulses to the far-end in order to meet synchronization between the TOE and the remote IT trusted product itself: this is necessary in the deployed network in order to assure secure environment for the intended usage of the TOE.

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided (FPT_RCV.2).

Automatic Recovery is applied in MPS115 switch when equipped with two redundant MSM Card in case of protection switchover event.

During normal operations the TSF, assigning Priority of Service for access to all shareable resources, ensures the TSF resource protection (FRU_PRS.2).

6.2 STRENGTH OF FUNCTION CLAIM FOR SECURITY FUNCTION

The TOE provides the following Security Function that is performed by permutational or probabilistic mechanism:

- User Authentication

User Authentication applies both for Manager User during authentication phase at a Management Interface and Subscriber User at Access Interface during authentication phase for self-affiliation facility.

The implementation provides the general strength of function of SOF-high for this SF.

6.3 ASSURANCE MEASURES

The purpose of this section is to show that the identified assurance measures ("AM") are appropriate to meet the security assurance requirements ("SAR") by mapping the identified assurance measures onto the assurance requirements.

The Assurance Measures that demonstrate the correct implementation of the Security Functions of the TOE are as follows:

- User Guidance (UG) Documentation
- Functional Specification (FSP) Document
- Security Policy Model (SPM) Document
- High Level Design (HLD) Document
- Low Level Design (LLD) Documentation
- Configuration Management Plan (CMP) Document
- Analysis of Testing (ATE) Document
- Security Functional Analysis (SFA) Document
- Vulnerability Assessment (VA) Document

6.3.1 USER GUIDANCE (UG)

AM	SAR	Description
UG.1	AGD_USR.1 AGD_ADM.1	Provides TOE users and administrators with procedural information on installation, configuration and management of the TOE
UG.2	ADO_IGS.1	Describes procedures for the installation, generation, and start-up of the TOE
UG.3	ADV_FSP.2	Detailed syntax information on the external interfaces used for such interaction with the TOE

6.3.2 FUNCTIONAL SPECIFICATION (FSP)

AM	SAR	Description
FSP.1	ADV_FSP.2	Describes the security functionality of the TOE
FSP.2	ADV_FSP.2	Defines the external interfaces to the TOE
FSP.3	ADV_RCR.1	Demonstrates correspondence with the ST

6.3.3 SECURITY POLICY MODEL (SPM)

AM	SAR	Description
SPM.1	ADV_SPM.1	Describes the security policy implemented by the TOE

6.3.4 HIGH LEVEL DESIGN (HLD)

AM	SAR	Description
HLD.1	ADV_HLD.2	Describes the relationship between TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces

HLD.2	ADV_RCR.1	Demonstrates correspondence with the FSP

6.3.5 LOW LEVEL DESIGN (LLD)

AM	SAR	Description
LLD.1	ADV_LLD.1	Describes the relationship between TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces
LLD.2	ADV_IMP.1	A source code representation of the TOE
LLD.3	ADV_RCR.1	Demonstrates correspondence with the HLD and TOE representation of implementation

6.3.6 CONFIGURATION MANAGEMENT PLAN (CMP)

AM	SAR	Description
CMP.1	ALC_LCD.1	Describes the development life-cycle model
CMP.2	ALC_DVS.1	Describes the security measures for the development site
CMP.3	ALC_TAT.1	Describes the development tools
CMP.4	ACM_AUT.1	Describes the CM model
	ACM_SCP.2	Describes how problem tracking is undertaken
CMP.5	ADO_DEL.2	Describes the delivery procedures and how they provide for the detection of modification
CMP.6	ACM_CAP.4	Description of TOE generation and acceptance procedures
CMP.7	ALC_FLR.1	Describes the way the discovered security flaws are handled

6.3.7 ANALYSIS OF TESTING (ATE)

AM	SAR	Description
ATE.1	ATE_DPT.1	Describes the testing undertaken of the TOE and the implementation of the functionality specified in the ST and the design documentation
ATE.2	ATE_COV.2	Describes coverage of the testing
ATE.3	ATE_FUN.1	Describes the testing of security functionality
ATE.4	ATE_IND.2	The TOE will be provided to the evaluators

6.3.8 SECURITY FUNCTIONAL ANALYSIS (SFA)

AM	SAR	Description

SFA.1	AVA_MSU.2	Describes vulnerability analysis undertaken
SFA.2	AVA_SOF.1	Strength of TOE security function evaluation

6.3.9 VULNERABILITY ASSESSMENT (VA)

AM	SAR	Description
VA.1	AVA_VLA.2	Identifies potential vulnerabilities in the TOE and provides a rationale as to why they are not exploitable in the intended environment for the TOE

7. RATIONALE

7.1 SECURITY OBJECTIVES RATIONALE

Policy/Threat/Assumptions	Objectives
Security Objectives for the TOE	
P.Audit_Review	O.Audit_Review
P.Default_Config	O.Trusted_Recovery, O.Audit_Generation
P.Info_Flow	O.Info_Flow, O.Domain_Separation, O.Correct_Routing
P.Need_to_Know	O.Access_Control
P.Notify	O.Alarm
T.Attack	O.Info_Flow, O.Domain_Separation, O.Correct_Routing
T.Audit_Corrupt	O.Audit_Protection
T.Breach	O.Info_Flow, O.Domain_Separation, O.Correct_Routing
T.Fail	O.Alarm, O.Trusted_Recovery, O.Fail_Secure
T.Unauth_Mgmt_Access	O.Trusted_Recovery, O.Audit_Review, O.Access_Control
Security Objectives for the Environment	
A.ADMIN-COMPETENT	OE.TRAINING, OE.AFFILIATION
A.ADMIN-DOCS	OE.TRAINING
A.ADMIN-NOEVIL	OE.TRUST
A.NETWORK_FRAGMENT	OE_NETWORK_FRAGMENT
A.POWER_SUPPLY	OE.POWER_SUPPLY
A.RELIABLE_TIME_STAMP	OE.RELIABLE_TIME_STAMP
A.SECURE_ENVIRONMENT	OE.SECURE_ENVIRONMENT, OE.POWER_SUPPLY

A.TRUSTED_GATEWAY	OE.TRUSTED_GATEWAY
P.Info_Flow	OE.TRUST

Table 12 Mapping the TOE Security Environment to Security Objectives

Objectives	**Policy/Threat/Assumptions**
Security Objectives for the TOE	
O.Access_Control	P.Need_to_Know, T.Unauth_Mgmt_Access
O.Alarm	P.Notify,T.Fail
O.Audit_Generation	T.Attack, P.Default_Config
O.Audit_Protection	T.Audit_Corrupt
O.Audit_Review	P.Audit_Review, T.Unauth_Mgmt_Access
O.Correct_Routing	P.Info_Flow, T.Attack, T.Breach
O.Domain_Separation	P.Info_Flow, T.Attack, T.Breach
O.Fail_Secure	T.Fail
O.Info_Flow	P.Info_Flow, T.Attack, T.Breach
O.Trusted_Recovery	P.Default_Config,T.Fail, T.Unauth_Mgmt_Access
Security Objectives for the Environment	
OE.AFFILIATION	A.ADMIN-COMPETENT
OE.NETWORK_FRAGMENT	A.NETWORK_FRAGMENT
OE.POWER_SUPPLY	A.POWER_SUPPLY, A.SECURE_ENVIRONMENT
OE.RELIABLE_TIME_STAMP	A.RELIABLE_TIME_STAMP
OE.SECURE_ENVIRONMENT	A.SECURE_ENVIRONMENT
OE.TRUSTED_GATEWAY	A.TRUSTED_GATEWAY

OE.TRAINING	A.ADMIN-COMPETENT, A.ADMIN-DOCS
OE.TRUST	A.ADMIN-NOEVIL, P.Info_Flow

Table 13 Tracing of Security Objectives to the TOE Security Environment

7.1.1 POLICIES

P.Audit_Review: Audit Review

In General, P.Audit_Review is addressed by:

1. O.Audit_Review: Audit Review Information. The TSF must provide the capability to review and analyze audit information.

P.Default_Config: Default Configuration

Coverage Rationale:

O.Trusted_Recovery supports P.Default_Config by ensuring the recovery to a secure state after a failure

O.Audit_Generation upholds P.Default_Config by ensuring, as a default of the TOE, the generation of all the security relevant events.

In General, P.Default_Config is addressed by:

1. O.Trusted_Recovery: Recovery Security State. Ensure the recovery to a secure state, without security compromise, after a discontinuity of operations. Ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the network.
2. O.Audit_Generation: Audit Records Generation. Ensures the generation of all the security relevant events.

P.Info_Flow: Flow of Information

Coverage Rationale:

The objective O.Info_Flow will provide complete coverage as it specifies the requirements by which all information flows, both inwards and outwards, are controlled and handled

In General, P.Info_Flow is addressed by:

1. O.Info_Flow: Information Flow Control. The TOE must ensure that any information flow control policies are enforced
2. O.Domain_Separation: The TOE must ensure the separation of Subscriber, Gateway, PVC and sPVC Connections and Management Data flow
3. O.Correct_Routing: The TOE will correctly route traffic according to the switching parameters specified at connection set-up time in order to keep all the data associated to Subscriber Users, Gateways, PVC and sPVC Connections separated one each other
4. OE.TRUST: Those responsible for the TOE must ensure that only highly trusted users are given privileges that enable them to modify the security configurations of the TOE.

P.Need_to_Know: User Need to Know

Coverage Rationale:

O. Access_Control ensures that the TSF enforces the restrictions to resources defined by the authorized users, thereby implementing the policy P.Need_to_Know.

In General, P.Need_to_Know is addressed by:

1. O.Access_Control: Access Control Policy. The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions. The access is based on Access Control Policy.

P.Notify: Notification of Failure

Coverage Rationale:

O.Alarm supports P.Notify by ensuring that the TOE will be capable of detecting and alerting of a failure or error with any component.

In General, P.Notify is addressed by:

1. O.Alarm: Alarm Notification for Security Risks. The TOE will be capable of detecting a failure or error with any component, hardware, software, or firmware. The TOE will provide alarming capabilities for notification of security related events and of a failure or error.

7.1.2 THREATS

T.Attack: Compromise of Information.

Coverage Rationale:

The objective O.Info_Flow will provide an effective countermeasure, as information flow control policies will be enforced.

The objective O.Domain_Separation will provide the separation between traffic and Manager Data flow.

The objective O.Correct_Routing will provide the separation of traffic data

In General, T.Attack is addressed by:

1. O.Info_Flow: Information Flow Control. The TOE must ensure that any information flow control policies are enforced
2. O.Domain_Separation: Separation of traffic and Management Data Flow. The TOE must ensure the separation of traffic and Management Data flow
3. O.Correct_Routing: Correct Routing of Traffic. The TOE will correctly route traffic according to the switching parameters specified at connection set-up time in order to keep all the traffic data separated one each other
4. O.Audit_Generation: Audit Record Generation. The TOE will provide the capability to generate readable audit data records associated to erroneous Manager user actions, erroneous or malicious Subscriber user actions or malicious unauthorized user actions in order to prevent unauthorized compromise of information.

T.Audit_Corrupt: Audit Data Corruption

Coverage Rationale:

By ensuring O.Audit_Protection, the threat T.Audit_Corrupt is countered because unauthorized access will be prevented and audit information will not be lost.

In General, T.Audit_Corrupt is addressed by:

1. O.Audit_Protection: Protect Audit Information. The TSF must provide the capability to protect audit information associated with individual users.

T.Breach: Transmission without Protection

Coverage Rationale:

The objectives O.Info_Flow will provide an effective countermeasure as: information flow control policies can be set to ensure that data protection is applied when appropriate

The objective O.Domain_Separation will provide the separation between traffic and Manager Data flow.

The objective O.Correct_Routing will provide the separation of traffic data

In General, T.Breach is addressed by:

1. O.Info_Flow: Information Flow Control. The TOE must ensure that any information flow control policies are enforced

2. O.Domain_Separation: The TOE must ensure the separation of traffic and Management Data flow

3. O.Correct_Routing: The TOE will correctly route traffic according to the switching parameters specified at connection set-up time in order to keep all the traffic data separated one each other

T.Fail: Component or Power Failure

Coverage Rationale:

O.Alarm mitigates the threat T.Fail by allowing for a quick response to correct the error or failure.

O.Trusted_Recovery mitigates the threat T.Fail by ensuring that the TOE will recover to a secure state, without security compromise, after a discontinuity of operations.

O.Fail_Secure helps to counter the threat T.Fail by ensuring that the TOE and the TSF can return to a secure state.

In General, T.Fail is addressed by:

1. O.Alarm: Alarm Notification for Security Risks. The TOE will be capable of detecting a failure or error with any component, hardware, software, or firmware. The TOE will provide alarming capabilities for notification of security related events and of a failure or error.

2. O.Trusted_Recovery: Recovery Security State. Ensure the recovery to a secure state, without security compromise, after a discontinuity of operations. Ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the network.

3. O.Fail_Secure: Preservation of Secure State for Failures. Preserve the secure state of the system in the event of a component or power failure.

T.Unauth_Mgmt_Access: Unauthorized Access

Coverage Rationale:

O.Trusted_Recovery mitigates the threat of T.Unauth_Mgmt_Access by ensuring that the TOE is able to return to a secure state after a discontinuity in operation.

O.Audit_Review mitigates the threat of T.Unauth_Mgmt_Access by making it known that actions are audited and reviewed on a periodic basis.

O.Access_Control counters the threat of T.Unauth_Mgmt_Access by limiting privileges through the implementation of an access control policy.

In General, T.Unauth_Mgmt_Access_ is addressed by:

1. O.Trusted_Recovery: Recovery Security State. Ensure the recovery to a secure state, without security compromise, after a discontinuity of operations. Ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the network.

2. O.Audit_Review: Review of Audit Records. The IT operating system will provide the capability to selectively view audit information. All Audit records will periodically be reviewed.

3. O.Access_Control: Access Control Policy. The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions. The access is based on Access Control Policy.

7.2 SECURITY REQUIREMENTS RATIONALE

7.2.1 FUNCTIONAL SECURITY REQUIREMENTS RATIONALE

Objectives for the TOE	Requirements
O.Access_Control	FDP_ACC.1, FDP_ACF.1, FIA_UAU.2, FIA_UID.2, FIA_AFL.1, FIA_SOS.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FDP_IFC.1, FDP_IFF.1, FTP_TRP.1 ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_SPM.1
O.Alarm	FPT_AMT.1, FPT_TST.1
O.Audit_Generation	FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FMT_MSA.3 ADV_FSP.2,ADV_HLD.2, ADV_LLD.1, ADV_SPM.1
O.Audit_Protection	FAU_STG.1, FAU_STG.4, FMT_MTD.1, FMT_SMR.1 ADV_SPM.1
O.Audit_Review	FAU_SAR.1, FMT_SMR.1, FMT_MTD.1 ADV_SPM.1, ADV_HLD.2, ADV_FSP.2
O.Correct_Routing	FDP_IFC.1, FDP_ITC.1, FTP_ITC.1
O.Domain_Separation	FDP_IFC.1, FPT_SEP.1, FTP_ITC.1
O.Fail_Secure	FPT_FLS.1
O.Info_Flow	FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FDP_UIT.1, FDP_ETC.2, FMT_MSA.3

O.Trusted_Recovery	FRU_FLT.1, FPT_RCV.2, FRU_PRS.2
Objectives for Operational Environment	**Requirements**
OE.AFFILIATION	AGD_ADM.1, AGD_USR.1, ADO_IGS.1
OE.NETWORK_FRAGMENT	AGD_ADM.1, AGD_USR.1
OE.POWER_SUPPLY	AGD_ADM.1, ADO_DEL.2, ADO_IGS.1
OE.SECURE_ENVIRONMENT	AGD_ADM.1, ADO_DEL.2, ADO_IGS.1
OE.RELIABLE_TIME_STAMP	AGD_ADM.1, AGD_USR.1
OE.TRAINING	AGD_ADM.1, AGD_USR.1, ADO_DEL.2, ADO_IGS.1
OE.TRUST	AGD_ADM.1
OE.TRUSTED_GATEWAY	AGD_ADM.1, AGD_USR.1

Table 14 Functional Components to Security Objective Mapping

O.Access_Control: Access Control Policy

Implementation Application:

O.Access_Control is implemented by FDP_ACC.1 and FDP_ACF.1 which define the access control policy, the subjects and objects which the policy covers, the security attributes that access to objects is based upon, and the rules of access between subjects and objects. The access control policy allows for the control of access to resources based on the user identity.

O.Access_Control is also implemented by FDP_IFC.1 and FDP_IFF.1 that define the information flow control policy enforced by TSF in order to check multiple presence of a self-affiliated Subscriber in the connected network.

FIA_UAU.2 require a user to be authenticated before any other TSF-mediation. This component traces back to and aids in meeting O.Access_Control.

FIA_UID.2 require a user to be identified before any other TSF-mediation. This component traces back to and aids in meeting O.Access_Control.

FIA_AFL.1 sets thresholds on the amount of attempts to logon that can be made before a user is locked out. This component traces back to and aids in meeting O.Access_Control.

FIA_SOS.1 defines a metric the authentication mechanism must meet. This component traces back to and aids in meeting O.Access_Control.

FMT_MSA.1 restrict the ability to modify object security attributes to authorized users. This component traces back to and aids in meeting O.Access_Control.

FMT_MSA.3 ensures that restrictive default values are defined for the security attributes used to enforce the security policies. This component traces back to and aids in meeting O.Access_Control.

FMT_SMR.1 specifies Manager Roles that are recognized by the TSF.

FTP_TRP.1 provides a trusted communication path to an authorized Manager user in order to supply authentication key to the TSF, be authenticated by TSF and establish a Manager user session with the TSF.

FTP_TRP.1 provides a trusted communication path to an authorized Subscriber user in order to supply authentication key to the TSF, be authenticated by TSF and access switching facilities.

The access control mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The access control policy [ADV_SPM.1] is also defined.

O.Access_Control is implemented in the TOE by:

1. FDP_ACC.1: Subset access control
2. FDP_ACF.1: Security attribute based access control
3. FDP_IFC.1: Subset information flow control
4. FDP_IFF.1: Simple security attributes
5. FIA_UAU.2: User authentication before any action
6. FIA_UID.2: User identification before any action
7. FIA_AFL.1: Authentication failure handling
8. FIA_SOS.1: Verification of secrets
9. FMT_MSA.1: Management of security attributes
10. FMT_MSA.3: Static attribute initialization
11. FMT_SMR.1: Security roles
12. FPT_TRP.1: Trusted Path
12. ADV_FSP.2: Fully defined external interfaces
13. ADV_HLD.2: Security enforcing high-level design
14. ADV_LLD.1: Descriptive low-level design
15. ADV_SPM.1: Informal TOE security policy model

O.Alarm: Alarm Notification for Security Risks

Implementation Application:

O.Alarm is implemented in the TOE by FPT_AMT.1 and FPT_TST.1, which require that tests are run to detect errors with the TSF.

O.Alarm is implemented in the TOE by:

1. FPT_AMT.1: Abstract machine testing
2. FPT_TST.1: TSF testing

O.Audit_Generation: Audit Records Generation

Implementation Application:

FAU_GEN.1 outlines what data must be included in audit records and what events must be audited.

FAU_GEN.1 is necessary to generate audit record.

FAU_GEN.2: Security-relevant actions must be associated with individual users.

FMT_MSA.3 outlines that, as a default, all the security relevant events are generated.

O.Audit_Generation is implemented by FPT_STM.1, which requires the capture of the accurate time, which can be associated with the audited event. The audit mechanism is described in terms of its purpose [ADV_FSP.2], its external interfaces [ADV_HLD.2], and its internal interfaces [ADV_LLD.1]. The audit policy [ADV_SPM.1] is also defined.

O.Audit_Generation is implemented in the TOE by:

1. FAU_GEN.1: Audit data generation
2. FAU_GEN.2: User identity association
3. FPT_STM.1: Reliable time stamps
4. FMT_MSA.3: Static Attribute Initialization
5. ADV_FSP.2: Fully defined external interfaces
6. ADV_HLD.2: Security enforcing high-level design
7. ADV_LLD.1: Descriptive low-level design
8. ADV_SPM.1: Informal TOE security policy model

O.Audit_Protection: Protect Audit Information

Implementation Application:

FAU_STG.1 is chosen to ensure that the audit trail is always (i.e., from initial start-up) protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail.

FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full and resources will not be compromised upon recovery.FAU_STG.4 is necessary to prevent the loss of audit records when the audit storage is full.

O.Audit_Protection is implemented by FMT_MTD.1 covers the requirement that audit data be available for review by ensuring that users, other than Administrator, cannot delete audit logs.

FMT_SMR.1 defines the Manager Roles available at the TOE Management Intefaces as used by TSF in order to enforce Access Control Policy while accessing from outside of the TOE the content of the buffer used to store and protect audit records.

O.Audit_Protection is implemented in the TOE by:

1. FAU_STG.1: Protected audit trail storage
2. FAU_STG.4: Prevention of audit data loss
3. FMT_MTD.1: Management of TSF Data
4. FMT_SMR.1: Security roles
5. ADV_SPM.1: Informal TOE security policy model

O.Audit_Review: Review of Audit Records

Implementation Application:

FAU_SAR.1 implements O.Audit_Review by requiring the review of audit records. The audit policy [ADV_SPM.1] includes a description of the facilities available at the interface [ADV_HLD.2] to review audit data [ADV_FSP.2].

O.Audit_Review is implemented by FAU_SAR.1, which require easy interpreting format of audited events.

FMT_SMR.1 defines the Manager Roles available at the TOE Management Interfaces that are allowed to periodically review audit records.

FMT_MTD.1 defines the scope of Manager Roles available at the TOE Management Interfaces in order to clera the buffer used to maintain the information used for audit review.

O.Audit_Review is implemented in the TOE by:

1. FAU_SAR.1: Audit review
2. FMT_SMR.1: Security roles
3. FMT_MTD.1: Management of TSF Data
2. ADV_SPM.1: Informal TOE security policy model
3. ADV_HLD.2: Security enforcing high-level design
4. ADV_FSP.2: Fully defined external interfaces

O.Correct_Routing: Correct Routing of Traffic

Implementation Application:

O.Correct_Routing: the correct routing is based on the information flow control polices security attributes defined as per the component FDP_IFC.1.

O.Correct_Routing is provided by FDP_ITC.1, which provide the means of controlling the reception of information without security attributes

O.Correct_Routing is provided by FTP_ITC.1, which provides a communication channel used by the TSF in order to terminate signalling traffic coming from a far-end IT entity and to generate signalling traffic towards a far-end IT entity.

O.Info_Flow is implemented in the TOE by:

1. FDP_IFC.1: Subset information flow control
2. FDP_ITC.1: Import of user data without security attributes
3. FTP_ITC.1: Inter-TSF trusted channel

O.Fail_Secure: Preservation of Secure State for Failures.

Implementation Application:

O.Fail_Secure is implemented in the TOE by FPT_SEP.1, FPT_RCV.2, FPT_FLS.1 and FRU_FLT.1, which ensure that the TOE can return to a secure state.

O.Fail_Secure is implemented in the TOE by:

1. FPT_RCV.2: Automated recovery
2. FRU_FLT.1: Degraded fault tolerance
3. FPT_SEP.1: TSF Domain Separation
4. FPT_FLS.1: Failure with preservation of secure state

O.Info_Flow: Information Flow Control

Implementation Application:

O.Info_Flow: the information flow control polices relating to the application of security functions, access control and archiving are defined and applied by the component FDP_IFC.1.

O.Info_Flow the information flow control polices relating to the application of security functions, access control and archiving are defined and applied by the component FDP_IFF.1.

O.Info_Flow is provided by FDP_ITC.1, which provide the means of controlling the information, which can be exchanged through imposition of the information flow control SFP.

O.Info_Flow is provided by FDP_UIT.1, which provide the transmission and reception of user data in a manner protected from modification errors.

O.Info_Flow is provided by FDP_ETC.2, which ensures the correct exporting of the Security Level of the Call and Security Level of Trunk Interface selected by the routing algorithm at connection set-up time and for all the lifetime of a switched connection.

O.Info_Flow is implemented in the TOE by:

1. FDP_IFC.1: Subset information flow control
2. FDP_IFF.1: Simple security attributes
3. FDP_ITC.1: Import of user data without security attributes
4. FDP_UIT.1: Data exchange integrity

O.Domain_Separation: Separation of Subscriber and Management Data Flow

Implementation Application:

O.Domain_Separation: the correct routing is based on the information flow control polices security attributes defined as per the component FDP_IFC.1.

O. Domain_Separation is provided by FPT_SEP.1, which provide the means of guarantee separation of security domains

O.Domain_Separation is provided by FTP_ITC.1, which provides a communication channel between the TSF and a far-end IT entity in order to let the control plane information flow across the TOE interfaces.

O.Domain_Separation is implemented in the TOE by:

1. FDP_IFC.1: Subset information flow control
2. FPT_SEP.1: TSF Domain Separation
3. FTP_ITC.1: Inter-TSF trusted channel

O.Trusted_Recovery: Recovery Security State

Implementation Application:

O.Trusted_Recovery is implemented in the TOE by FPT_RCV.2 which require the recovery to a secure state after a discontinuity of operation.

O.Trusted_Recovery is implemented in the TOE by FRU_PRS.2, which require full priority of service in accessing all shareable resources in TOE implementation.

O.Trusted_Recovery is implemented in the TOE as per FRU_FLT.1 by requiring the maintaining of all security functionalities, i.e. security state, except the ones performed by entities directly involved in a detected failure event.

O.Trusted_Recovery is implemented in the TOE by:

1. FPT_RCV.2: Automated recovery

2. FRU_PRS.2: Full priority of service

3. FRU_FLT.1: Degraded fault tolerance

OE.AFFILIATION

OE.AFFILIATION is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance
2. AGD_USR.1: User guidance
3. ADO_IGS.1: Installation, generation, and start-up procedures

The TOE environment must ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE.

OE.NETWORK_FRAGMENT

Implementation Application:

The procedures for administration [AGD_ADM.1] and secure use [AGD_USR.1] of the TOE must be documented.

OE.NETWORK_FRAGMENT is implemented in the TOE by:

1. AGD_ADM.1: Administrator Guidance
2. AGD_USR.1: User guidance

The TOE environment must ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE.

OE.POWER_SUPPLY

OE.POWER_SUPPLY is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance
2. ADO_DEL.2: Detection of modification
3. ADO_IGS.1: Installation, generation, and start-up procedures

Power supply system must be connected and configured in line with the developer's guidance documentation; administrators must ensure that the configuration remains in step with the ongoing developer's guidance.

OE.RELIABLE_TIME_STAMP

OE.POWER_SUPPLY is implmented in the TOE by:

1. AGD_ADM.1: Administrator guidance
2. AGD_USR.1: User guidance

The time reference in the TOE must be set in line with the developer's guidance and administrators must ensure that the configuration remains in step with the ongoing developer's guidance.

OE.SECURE_ENVIRONMENT

OE.SECURE_ENVIRONMENT is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance
2. ADO_DEL.2: Detection of modification
3. ADO_IGS.1: Installation, generation, and start-up procedures

The TOE must be installed and configured in line with the developer's guidance and administrators must ensure that the configuration remains in step with developer's ongoing guidance.

OE.TRAINING

Implementation Application:

The procedures for the secure delivery [ADO_DEL.2], installation [ADO_IGS.1], administration [AGD_ADM.1] and secure use [AGD_USR.1] of the TOE must be documented.

OE.TRAINING is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance
2. AGD_USR.1: User guidance
3. ADO_DEL.2: Detection of modification
4. ADO_IGS.1: Installation, generation, and start-up procedures

The TOE environment must ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE.

OE.TRUST

OE.TRUST is implemented in the TOE by:

1. AGD_ADM.1: Administator Guidance

The TOE environment must provide a mechanism that ensures that the likelihood of administration staff performing illegal actions is minimised.

Those responsible for the TOE security functions will be supplied with an accurate guide addressing the correct administration of security relevant aspects.

OE.TRUSTED_GATEWAY

OE.TRUSTED_GATEWAY is implmented in the TOE by:

3. AGD_ADM.1: Administrator guidance

4. AGD_USR.1: User guidance

The TOE must be connected at Gateway Interfaces with trusted, non-hostile IT Product in line with Administrator and User guidance documentation

7.2.2 STRENGTH OF FUNCTION RATIONALE

The operational environment for the TOE is characterized by the potential presence of unauthorized users possessing a high potential of attack conducted both from the Management Interface and Access Interface in order to access Management Data and switching facility respectively.

The TOE has been designed with password mechanisms and embedded automatic account locking features that provides adequate protection against deliberately planned or organized breach of TOE security.

The Lockout Admin Role is the only Manager Role which is able to reset a locked account for Manager user.

The Manager and Global are the only Manager Role which are able to reset a locked account for Subscriber user.

The operational environment for the TOE is characterized by the presence of no-evil, high trusted Administrator as well, provided with accurate security guidance documentation and enforcing regular policies of checking audit record collected from the TOE associated to hacking attempts.

The claiming of a password of at least 8 characters for Lockout Admin Role, case sensitive and picked up form the sets {A-Z}, {a-z} and {0-9} leads to (26+26+10) raised to the power of 8 different combinations for the Lockout Admin Role, which is not involved in locking account mechanisms.

So, a probability of 1 out of 218,340,105,584,896 is computed to guess the secrect in the worst case for Lockout Admin Role.

In this hypotesis, the claim of SOF-high seems to be appropriate for intended usage.

7.3 JUSTIFICATION OF ASSURANCE LEVEL

The Security Objectives allocated to the TOE have been defined for military, mission-critical application in which high system reliability is claimed and demanded.

Security Objectives claimed for the TOE require a methodic, documented design and development approach, supported by a well-defined life-cycle model and review policies together with automatic procedures for the managements of items under configuration control; at the same time they require a well-define test approach with particular care to malfunction managements.

Moreover a secure Product is a Product designed and implemented in a secure development environment that puts particular attention in all the aspects that may affect the quality and reliability of the Product.

In order to meet Security Objectives for the Environment and assure secure network design and deployment, well-defined and documented installation procedures are required and detailed Administrator and User Guidance must be provided to those responsible for the TOE in the Operational Environment.

For all those reasons, the choice for Evaluation Assurance Level EAL4, as specified in Common Criteria for Information Technology Security Evaluation, Version 2.1 (ISO/IEC 15408), seems to be the more appropriate for meeting the claimed security needs for the Product.

Moreover, augmenting the claims with Flaw Remediation components, as specified in Common Criteria for Information Technology Security Evaluation, Version 2.1 (ISO/IEC 15408), puts in evidence the necessity and particular care in addressing in the correct way security flaw management, in terms of prevention and corrections of malfunctions reported from the Operational Environment at Customer Site.