MICROSENS

100G Encryption Module

Overview

100G Encryption Module is a part of MICROSENS MSP3000 Platform, a high performance and flexible carrier-class transmission system. The MSP3000 Platform enables increasing transport capacities in CWDM, DWDM and SDH networks. The use of wide range TDM modules permits to reduce the number of necessary wavelengths and to decrease the overall cost of the application. Ethernet over SDH modules enable using existing SONET/SDH infrastructure for IP transmission.

The general features of the system:

- 19" 2U Chassis with 6 module slots and management card
- 19" 7U Chassis with 20 module slots and management card
- Hot swappable modules & power supplies
- Redundant power supplies with -48 VDC input (opt. 230 VAC)
- Exchangeable air- and filter module
- Wide range of functional xWDM and TDM modules available

The functional modules of MSP3000 Platform include:

- 10G/100G/200G TDM modules
- 10/100G transponders
- Dedicated family for DCI applications
- 10G protocol converter 10G LAN to 10G WAN (OC-192/STM-64)
- DWDM MUX/DeMUX, OADMs, EDFAs, ROADM, Fiber monitoring, etc

Introduction

MICROSENS 100G Encrytpion module is is a HW platform allowing aggregation, encryption and transport of ten signals (10GbE, 8GFC, 10GFC, 16GFC, STM64/OC192, OTU2, OTU1e or OTU2e) over a G709 OTU4 line interface.

Features

- Line Encryption based on GCM AES-256 algorithm with Diffie Hellman keys exchange
- Ten Multiprotocol client port interfaces
    - 10GbE
    - 8GFC
    - 10GFC
    - 16GFC
    - STM64/OC192
    - OTU2
    - OTU1e
    - OTU2e
- SFP+ modules for client port physical interfacing
- Standard G709 OTU4 Line interface
- QSFP28 module for line port physical interfacing
- DDM (Digital Diagnostic Monitoring) information from SFP+ and line transceiver

System description

The Encryption card is made of 2 groups of 5 SFPs spread as following:

Group 1: Client ports 1, 2, 3, 4 and 9

Group 2: Client ports 5, 6, 7, 8 and 10

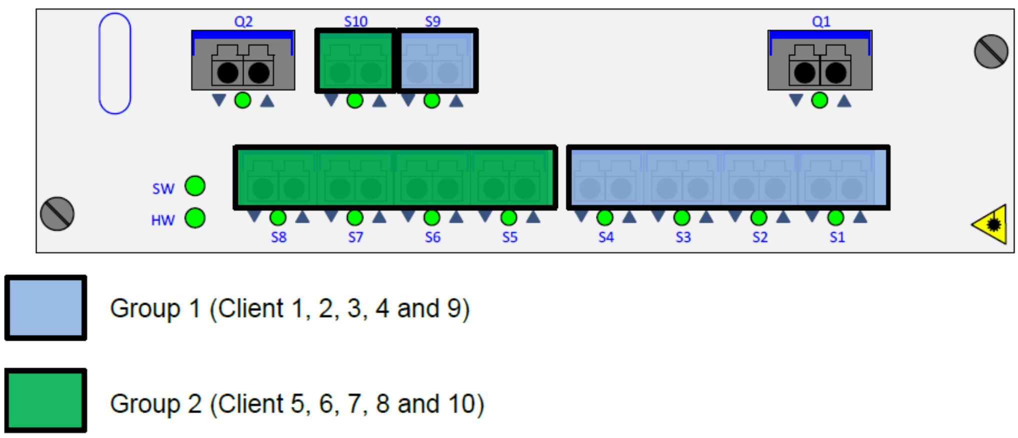

Figure 1 Group/SFP+ Allocation

Each group of 5 ports can be configured in the following protocol mode:

- 5 x MP
- 4 x EMP
- 2 x MP + 2 x 16GFC
- 3 x 16GFC

A Multi-protocol (MP) port can support the following protocols:

- 8GFC
- OC192/STM64
- 10GbE

An Enhanced Multi-protocol (EMP) port can support the following protocols:

- 8GFC
- OC192/STM64
- 10GbE
- 10GFC
- OTU2
- OTU1e
- OTU2e
- MICROSENS Wrapper (11.09 Gb/s)

The following table provides the port used upon the select mode:

	Client port 1	Client port 2	Client port 3	Client port 4	Client port 9
	Client port 5	Client port 6	Client port 7	Client port 8	Client port 10
5 x MP	MP	MP	MP	MP	MP
4 x EMP	EMP	EMP	EMP	EMP	OOS (1)
2 x MP + 2 x 16GFC	16GFC	16GFC	MP	MP	OOS (1)
3 x 16GFC	16GFC	16GFC	16GFC	OOS (1)	OOS (1)

(1) OOS : Out Of Service (the port is not used).

Additionally, if the Group 1 and Group 2 are both configured in 3 x 16GFC mode, an additional 16GFC client port is enabled (Client port 4) and the encryption card can transport 7 x 16GFC protocols.

In that case, the client ports of the Group 1 and Group 2 will be configured as following

Group	Group 1					Group 2				
Client Port	1	2	3	4	9	5	6	7	8	10
Protocol	16GFC	16GFC	16GFC	16GFC	OOS	16GFC	16GFC	16GFC	OOS	OOS

The block diagram for the Encryption module is given in Figure 2.

The Encryption module is a bi-directional device. It therefore has different sections:

- Upstream Section: from ten multi protocol optical input to G709 OTU4 optical output
- Downstream Section: from G709 OTU4 optical input to ten multi protocol optical output
- Common sections composed of :
    - Controller block, providing interfacing to the chassis controller board hosting the SNMP Agent.
    - Power supplies: generates different internal power supplies from the -48V – input
    - Front panel LEDs indicating the status of the ports, line and the Encryption module common functions

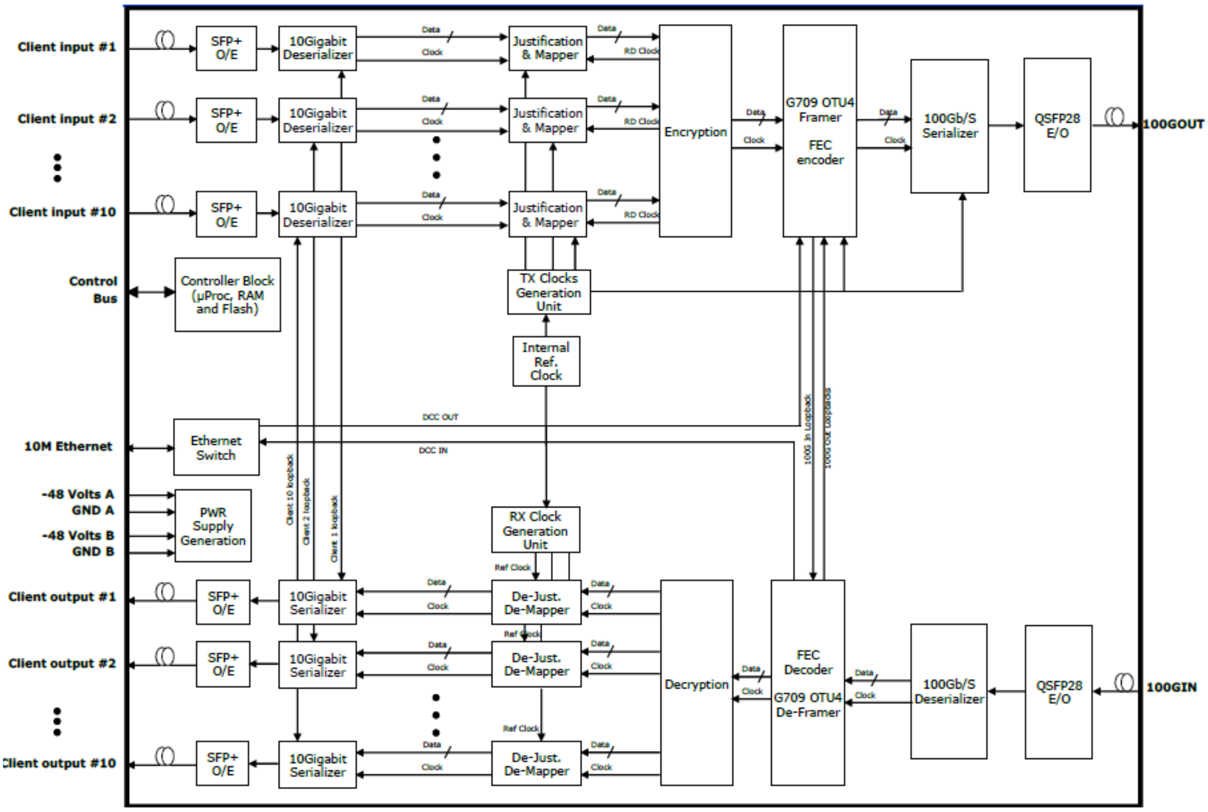

Figure 2: Block diagram.

Upstream section

Input Ports interfacing

The upstream section has up to ten client inputs.

Client physical interfacing is done through standard SFP+ modules.

The upstream client port (independently of the configured protocol) is forwarded to the mapper block.

The following information is provided to the controller:

- SFP+ absence
- Loss of optical input signal
- Loss of synchronization on incoming signal:

Protocol	Loss of Synchronisation description
8GFC	Loss of 10b/8b decoder sync
OC192/STM64	Loss of Frame
10GbE	Loss of 66B/64B decoder sync
10GFC	Loss of 66B/64B decoder sync
OTU2	Loss of Frame
OTU1e	Loss of Frame
OTU2e	Loss of Frame
MICROSENS Wrapper	Not available
16GFC	Loss of 66B/64B decoder sync

- Counting of incoming errors:

Protocol	Error counter description
8GFC	FCS Error
OC192/STM64	B1 Error
10GbE	FCS Error
10GFC	FCS Error
OTU2	Not available
OTU1e	Not available
OTU2e	Not available
MICROSENS Wrapper	Not available
16GFC	FCS Error

- DDM information

Mapper

Incoming signals must be synchronized together and are mapped in a proprietary frame prior of being multiplexed together for framing in a 10.709 Gb/s (11.09Gb/s for the MS430687/8M) signal.

For each client input signal, three different types of justification can be performed:

- Null Justification (0): the default mapping is used
- Negative Justification (-2): two data bytes are added to the default mapping.
- Positive Justification (+2): two data bytes are replaced by justification bytes in the default mapping.

Incoming Telecom client signals (OC12/STM4 and OC48/STM16) frequencies have a tolerance of ±20 ppm. Incoming Datacom client signals (GbE, 1GFC, 2GFC and 4GFC) frequencies have a tolerane of ±100 ppm. Local system clocks have a tolerance of ±20 ppm.

The justification process ensures that the clock frequency of the client data stream restored at the far end will be the one of the initial incoming client signals (±20 ppm or ±100 ppm).

The justification process is performed for each incoming client.

Synchronized incoming signals are mapped in a proprietary frame. This frame transports the following information in addition to the data (per client port):

- Client Signal Fail indication: a bit in the mapping frame is set in case one of the following conditions are present on the incoming signal (see Figure 2)

    - SFP not present
    - Loss of incoming signal.
    - Loss of synchronization
    - Justification buffer overflow

A client BIP-8 parity (CBIP) is computed over each mapped client signal and inserted in the corresponding mapping frame.

The following information is provided to the controller on a per port basis:

- Client Signal Fail asserted
- Justification buffer overload

RMON (Remote Network Monitoring)

Remote Network Monitoring functionality is provided on the 10GbE, 10GFC and 16 incoming client port. The upstream client port is 66B to 64B decoded to provide the RMON statistics.

The following statistics are made available on a per port basis:

- Packet counters:

Total number of packets (including, broadcast packets, and multicast packets) received

- CRC errors counter

Total number of packets received that either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Mapper

Incoming signals must be synchronized together and are mapped in a proprietary frame prior of being multiplexed together for framing in a G709 OTU4 signal.

Synchronisation is performed thanks to a justification process which can tolerate ±100 ppm frequency deviation to the nominal client protocol bit rate

The mapper inserts additional information:

- Client Signal Fail indication: a bit in the mapping frame is set in case one of the following conditions are present on the incoming signal (see Figure 3)
  - SFP+ not present
  - Loss of incoming signal.
  - Loss of synchronization on incoming signal
  - Justification buffer overflow

The following information is provided to the controller on a per port basis:

- Client Signal Fail asserted
- Justification buffer overload

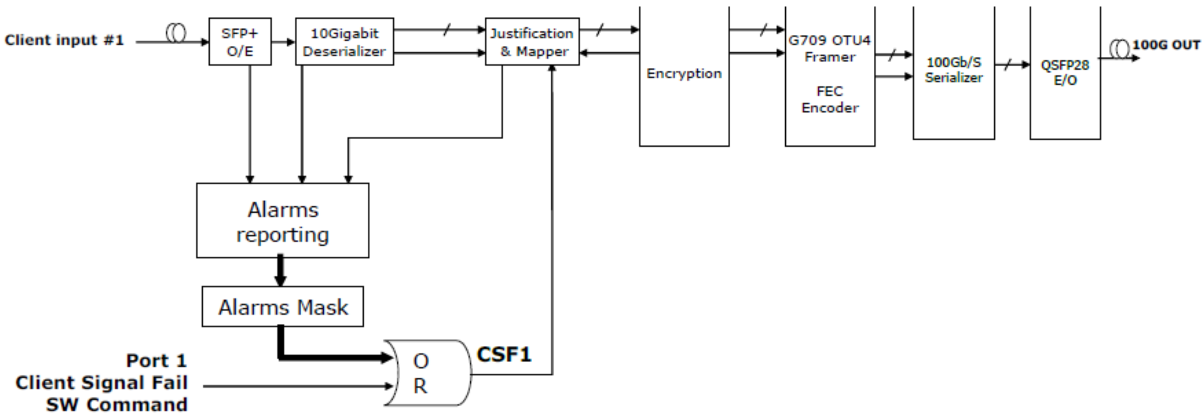

Figure 3: Upstream Client Signal Fail assertion principle.

Encryption

The ten mapped client signals coming from the Mapper are then interleaved in an OPU4 container which is encrypted. Encrypted data are then transmitted to the framer.

G709 OTU4 Framer

The encrypted signal is then inserted in a G709 ODU4 payload.

The payload is framed into a G709 OTU4 output signal.
SM-BIP8 is calculated and inserted in its corresponding locations in the outgoing signal. The following information is provided to the controller on a per port basis:

- SM-BDI inserted

FEC encoder

Standard G709 OTU4 G-FEC encoding is performed and inserted in dedicated bytes of the G709 OTU4.

10M DCC

The 10M DCC allows inserting a 10Mb/s Ethernet data communication channel coming from the Ethernet switch and transported in the G709 OTU4 frame.

It is inserted in unused bytes of the G709 OTU4 frame.
The following maintenance actions can be set on the Framer

- 100G Facility Loopback
- 100G Terminal Loopback

Line Optical Interfacing

Line optical interfacing is performed through QSFP28 modules.

The following alarms can be read from the Line Optical Interface:

- Transmitter fault
- DDM information

The following parameters can be configured on the QSFP28:

- Shut down optical transmitter

DownStream Section

Line Optical Interfacing

Line optical interfacing is performed through QSFP28 modules.

The following alarms can be read from the Line Optical Interface:

- Loss of input signal (OPS2e dLOS-P)
- DDM information

G709 OTU4 De-Framer

G709 OTU4 frame alignment is performed, FEC decoding is performed (see below) and SM-BIP8 parity calculation is computed.

The following information is provided to the controller for the G709 OTU4 incoming signal:

- Loss of Frame on incoming signal
- SM-IAE received
- SM-BDI received
- SM-BIP8 errors counting
- G709 OTU4 FEC corrected errors counting

10M DCC

The 10M DCC allows giving access to a 10Mb/s Ethernet data communication channel transported in the G709 OTU4 frame. It is extracted unused bytes of the G709 OTU4 frame and passed to the Ethernet switch.

FEC decoder

Standard G709 OTU4 G-FEC decoding is performed and FEC corrected errors counting is performed

Decryption

The data coming from the De-Framer are decrypted and the data contained in the OPU4is then transmitted to each de-mapper.

De-Mapper

The de-mapper extracts client data and the de-justification process allows recovering the client data stream mapped at the far end.

Client Signal Fail information is also extracted and reported to the controller block (see Figure 4). Under failure conditions, an output client AIS (CAIS) signal is inserted on the outgoing client port.

The alarms leading to assertion of client AIS are:

- Loss of optical input signal
- Loss of Frame on G709 OTU4 input.
- SM-IAE received on the G709 OTU4 input.
- Incoming CSF detected
- De-mapper buffer overflow

The client AIS signal when asserted shuts down the client optical output.
The CAIS mechanism is described in Figure 5.

The following information is provided to the application processor on a per port basis:

- CSF received
- BIP-8 errors counting
- CAIS asserted

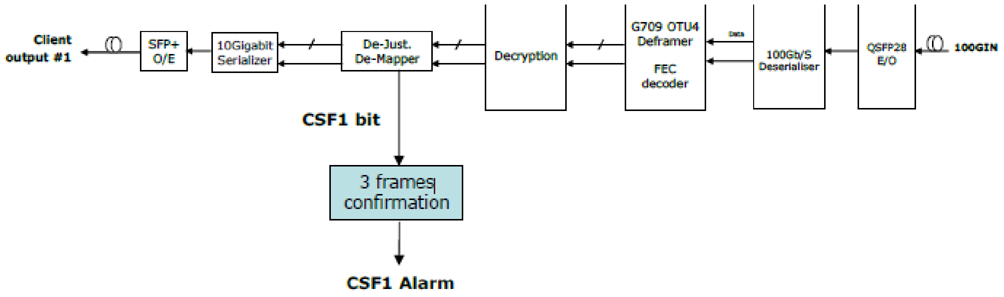

Figure 4: Downstream CSF detection mechanism

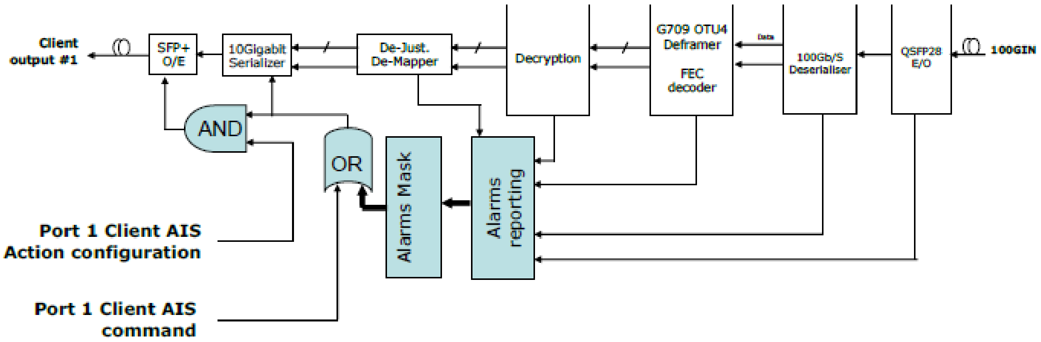

Figure 5: Downstream CAIS mechanism (with 2x10G).

Output RMON and output port interfacing

The data is serialized and converted to an optical signal by an SFP+ Transceiver.

The following information is provided to the control block:

- Optical transmitter failure
- DDM information.

The following configuration information is received from the control block on a per port basis:

- Optical output shut-down

RMON (Remote Network Monitoring)

Remote Network Monitoring functionality is provided on the 10GbE, 10GFC and 16GFC outgoing client port. The downstream client port is 66B to 64B decoded to provide the RMON statistics.

The following statistics are made available on a per port basis:

- Packet counters:

Total number of packets (including, broadcast packets, and multicast packets) transmitted

- CRC errors counter

Total number of packets transmitted that either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Encryption/Decryption

The encryption mechanism is based on the GCM AES-256 algorithm with Diffie-Helman key exchange. The public authenticating key used in the Diffie-Helman mechanism is not stored anywhere in the system (Encryption module or Management board) for security reason. As a consequence, on module reset, the Public key must be defined again.

The same public authenticating key must be defined on the two Encryption cards connected one to each other.
The Encryption module is able to protect the traffic against many hacking attack like Man-in-the-middle, Brute force, Replay attack, etc…)

A user with Crypto Officer role has access to the following features:

- Configuration
  - Public authenticating key definition
  - Session key lifetime in seconds from 1 to 86400 seconds (default is 60 seconds)
  - Force key exchange
  - Reset monitoring information
- Monitoring
  - Crypto Officer login history on each Encryption module
    - last successful login
    - last failed login
    - failed login count
  - Session Key history on each Encryption module
    - Session key time remaining
    - Last failed key exchange
    - Failed key exchange count
    - Encryption off time remaining
    - Elapsed Time Since Last Monitoring Reset

Among these features, a user with Crypto User role has only access to the monitoring information.

Maintenance Loop backs

Client Terminal Loopback

As a test feature, an individual Client Terminal Loopback can be performed for maintenance operations. The client signal extracted from the line input signal is looped back to the line output signal. The description of the data path in case of Client Terminal Loopback is described on Figure 6

Client Facility Loopback

As a test feature, an individual Client Facility Loopback can be performed for maintenance operations. The client signal received on an input port is looped back on the corresponding outgoing client port. The description of the data path in case of Client Facility Loopback is described on Figure 7

Line Terminal Loopback

As a test feature, a Line Terminal Loopback can be performed for maintenance operations, allowing looping back the transmitted 100Gb/s signal on the downstream section. The description of the data path in case of Line Terminal Loopback is described on Figure 8

<u>Line Facility Loopback</u>

As a test feature, a Line Facility Loopback can be performed for maintenance operations, allowing looping back the received 100Gb/s signal on the upstream section. The description of the data path in case of Line Facility Loopback is described on Figure 9.

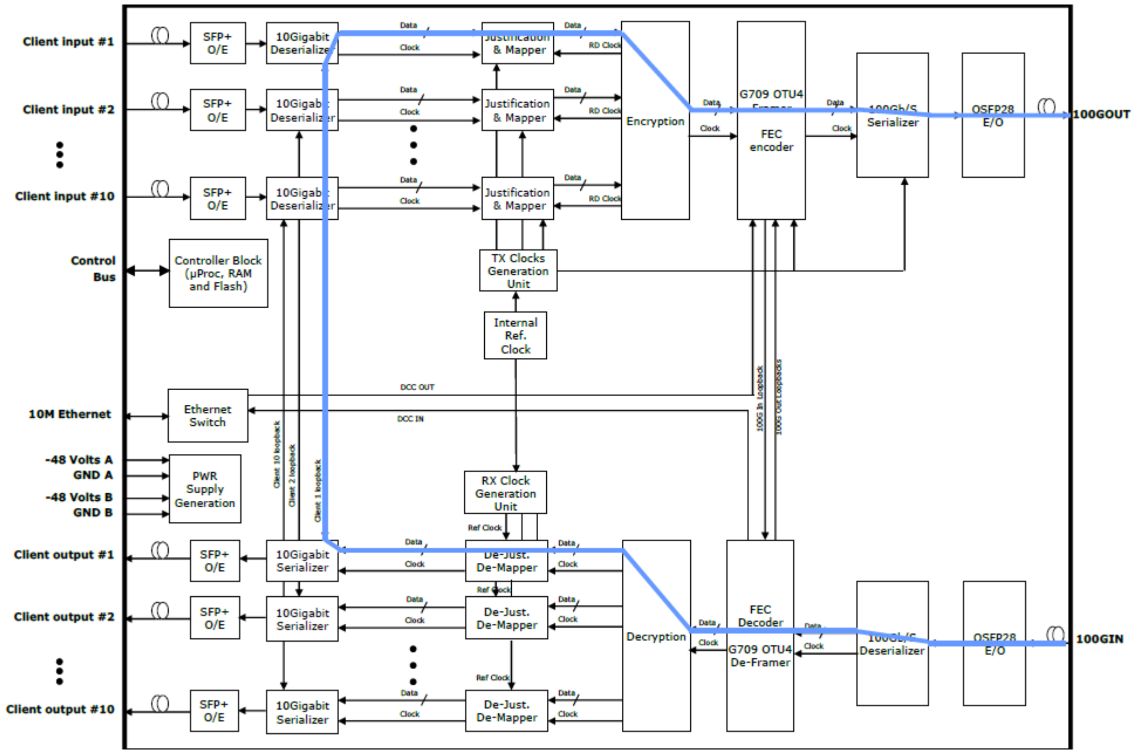

Figure 6: Signal data path in Client Terminal Loopback operation.

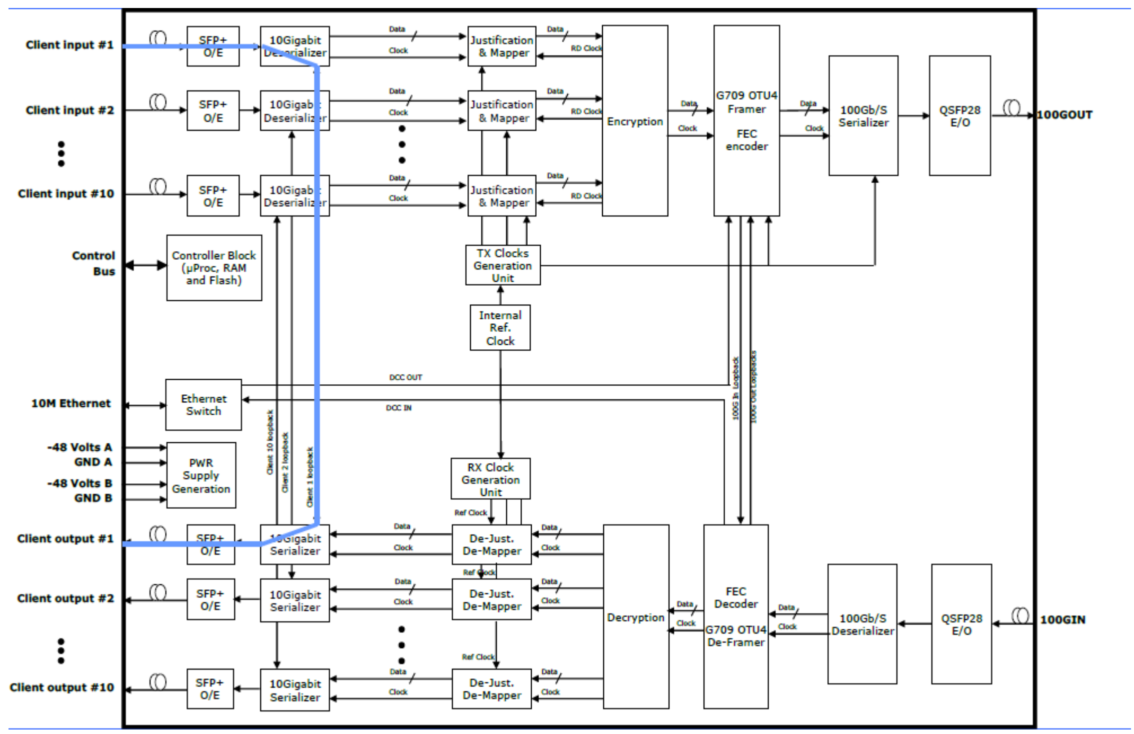

Figure 7: Signal data path in Client Facility Loopback operation

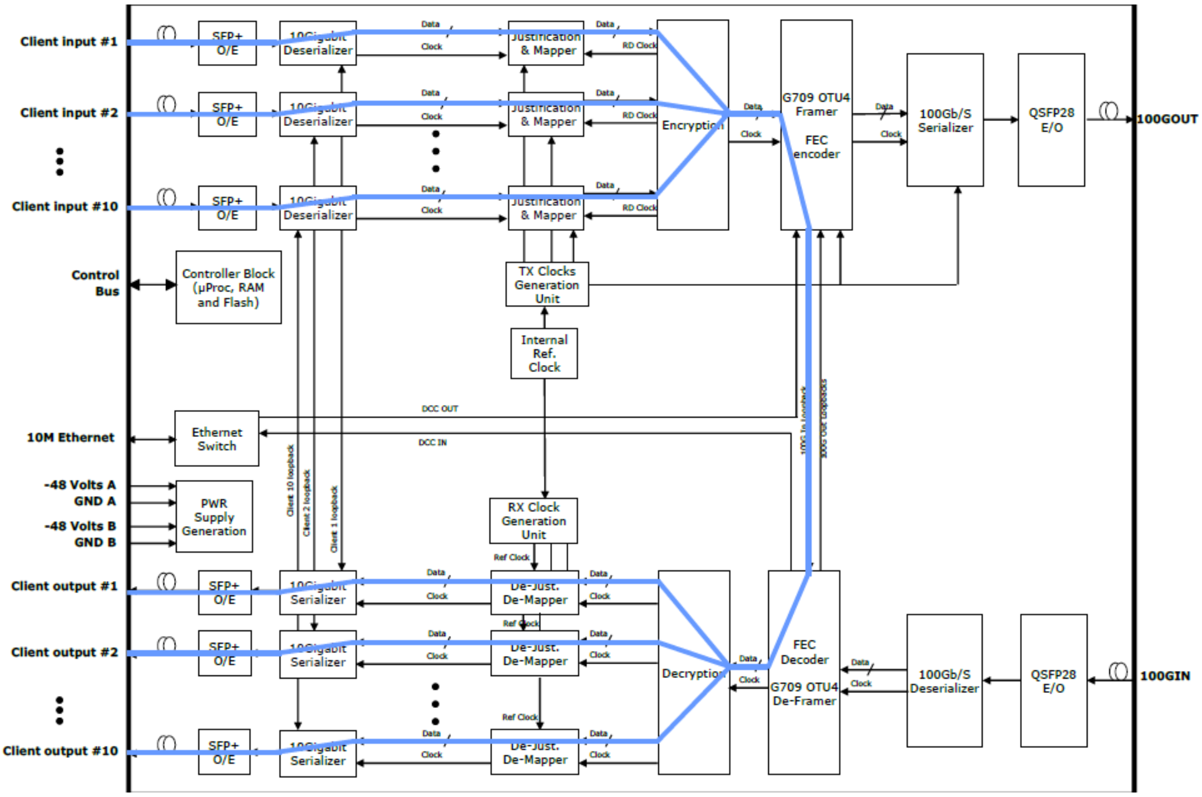

Figure 8: Signal data path in Line Terminal Loopback operation.

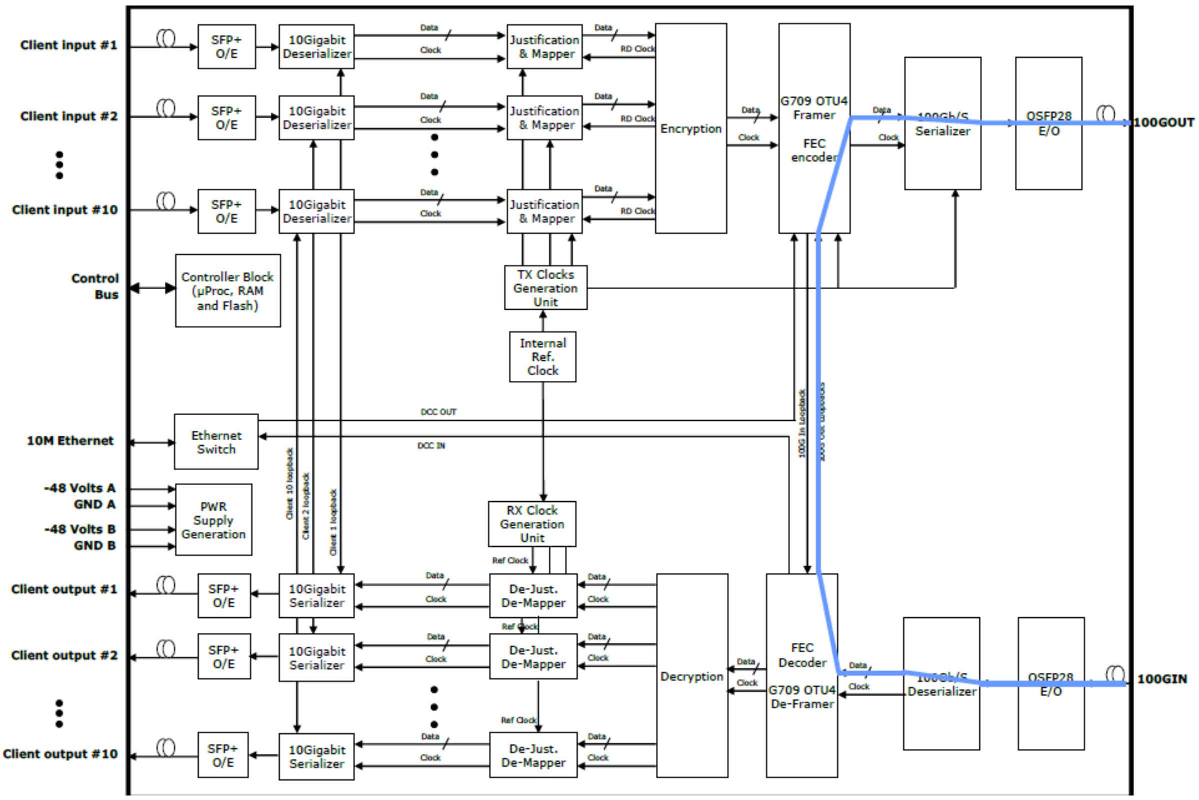

Figure 9: Signal data path in Line Facility Loopback operation

Clock Generation Unit

DownStream Clock Generation Unit

The DownStream Clock generation unit generates all internal clock signals required by the downstream part of the Encryption module.

It generates in particular the reference clocks which are fed to the individual de-mappers. This reference clock is defined according to the selected protocol as following:

Protocol	Reference Clock
8GFC	8.5 GHz
OC192/STM64	9.95328 GHz
10GbE	10.3125 GHz
10GFC	10.5184 GHz
OTU2	10.709225 GHz
OTU1e	11.0491 GHz
OTU2e	11.09572 GHz
MICROSENS Wrapper	11.0592 GHz
16GFC	14.25 GHz

The following information is made available to the controller block:

- DownStream clock recovery unit not locked

Controller Block

The controller block is composed of a microprocessor associated with Flash and RAM memories.

The controller block collects information from different functional blocks and configures the HW according to a configuration file received.

The raw information (alarms, monitoring, inventory …) generated by the HW are processed by the microprocessor and delivered to the Management Unit as high level consolidated data.

Out of Service and In Service states

Client port

An individual command is accessible to set the client port Out of Service.

When the client port is Out of Service, an Out of Service information is sent over the line interface to inform the far end client port that the local client port is Out of Service. The client port provides the following additional information:

- Local OS: The local client port is Out of Service

An Out of Service client port has the following behaviour

- The SFP+ Laser is be shut down
- All the alarms of the client port are masked (except Local OS and Distant OS).
- All the counters of the client port are disabled (the invalid bit is set).

- All the SFP+ measures of the client port are disabled (the value is set to 0).

When the client port is In Service, all the disabled features previously named are enabled again. The alarms are unmasked and the Out of Service information is not sent anymore over the line interface.

Line port
An individual command is accessible to set the line port Out of Service

Linked to the Out of Service state, the line port has the following additional information:

- Local OS: The local line port is Out of Service.

An Out of Service line port has the following behaviour:

- The 100G Line transmit Laser is shut down
- All the alarms of the line port are masked (except Local OS).
- All the counters of the line port are disabled (the invalid bit is set).
- All the 100G Line interfacing measures of the line port are disabled (the value is set to 0).

When the line port is In Service, all the disabled features previously named are enabled again and the alarms are unmasked.

Power Supplies

The power supply block generates from the received external -48 volts, the different internal supplies needed.

Interface Specifications

Client Interfaces Optical Characteristics

Client interfaces are provided by SFP+ transceivers. The optical characteristics are therefore given in the data sheet of the SFP+ plugged into the Encryption module.

Line Interface characteristics

Line interface is provided by QSFP28 transceivers. The optical characteristics are therefore given in the data sheet of the QSFP28 plugged into the Encryption module.

Appendixes

Laser Class

Laser Class	Risks	General Requirements
1	Considered safe to eye and Skin under all reasonably foreseeable conditions of operation.	Protective housing: may be required.

Module Leds description

LED	Status	Condition
SW	Green On	Normal
	Red On	SW Failure
HW	Green On	Normal
	Red ON	HW Failure
Line port (Q1)	Green	Normal
	Red	Link failure
100G Client port (Q2)	Green	Normal
	Red	Link failure
	OFF	Port not used
Client port (S1 to S10)	Green	Normal
	Red	Link failure
	OFF	Port not used

Front Panel Layout

The module occupies two slots in the chassis.

Client S1 to S10 is SFP+ cage capable of hosting standard SFP+ module
Line Q1 and Client Q2 is QSFP28 cage capables of hosting standard QSFP28 module.

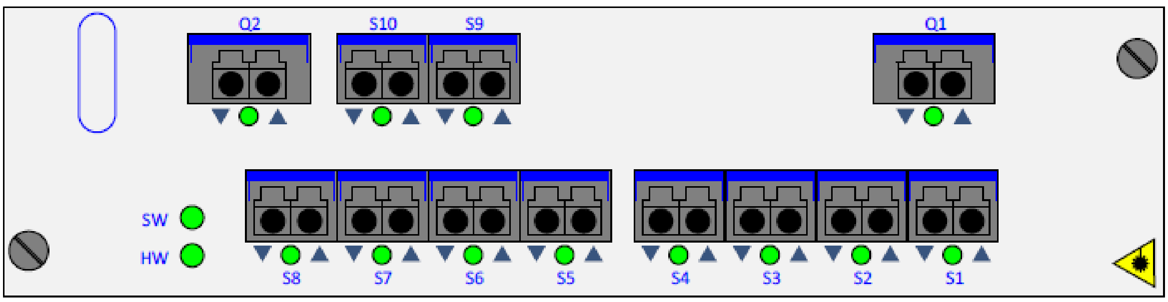

Figure 10: Front panel layout

Technical Specifications

Type	100G Encryption Module
Connectors	Local ports: SFP, Line ports: XFP or FFI
Line data rate	OTU4
Power consumption	<75W equipped with SFP+
Operating temp	-5°C to 50°C
Storage temp	-20°C to 85°C

Order Information

Art. No.	Description	Connectors
Modules		
MS430961M	Multirate Encryption-Module, 1x100GE/OTU4 (QSFP28) or 10xMultiprotocoal 16G FC/10GE/10G FC (SFP+) to encypteted OTU4 (QSFP28) (QSFP28 and SFP+ not included)	10x SFP+ 2x QSFP28

MICROSENS reserves the right to make any changes without further notice to any product to improve reliability, function or design. MICROSENS does not assume any liability arising out of the application or use of any product. pp\0919