सत्यमेव जयते

Ministry of Railways
Government of India

DRAFT SPECIFICATION FOR
Failsafe Networked Multiplexer (FNmux)

Specification No. RDSO/SPN/211/2012
Version 0.1 (Draft)

SIGNAL DIRECTORATE
RESEARCH DESIGNS & STANDARDS ORGANISATION
LUCKNOW-226011

DOCUMENT DATA SHEET			
Designation **RDSO/SPN/211/2012**			Version 0.1 (Draft)
Title of Document **Draft Specification for Failsafe Networked Multiplexer (FNmux)**			
Authors: **Akhilesh Yadav** **Designation: Director/Signal, RDSO**			
Approved by **Name: Shri Mahesh Mangal** **Designation: Sr. Executive Director/Signal, RDSO**			
Abstract This document defines specification for **Failsafe Networked Multiplexer (FNmux)**			

DOCUMENT CONTROL SHEET

NAME	ORGANISATION	FUNCTION	LEVEL
P. K. Bhagchandani	RDSO	Member	Prepare
Akhilesh Yadav	RDSO	Member	Prepare
Sh. Mahesh Mangal	RDSO	Approving Authority	Approve

AMENDMENTS

Specification No.	Version	Amendment	Amendment Details	Effective date
RDSO/SPN/211/2012	0.1	-	draft	-

1 SCOPE

1.1 This specification covers the technical and operational requirements of the Fail-SafeNetwork Mux for exchanging both vital and non-vital Signalling information using Dual redundant copper cable/OFC / radio communication media. Following types of signalling multiplexers are required to be used to replace signalling cables:

a) The Non Vital module having a 32 I/O will be responsible for transferring ofindication and other non-vital switch/relay status
b) The Vital module having a 8 I/O or 16 I/O configuration for transferring of vital point, signal, tracks and other similar vital relay status
c) A vital trackside function module for directly driving signals or points without any relay interface.

2 TERMINOLOGY

2.1 For the purpose of this specification, the terminology given in IRS: S23 and RDSO/ SPN/ 144/2006 shall apply.

3 APPLICABLE DOCUMENTS

4

SN	Subject	Spec
1	EN 50126	Railway Applications-Specifications and demonstration of Reliability, Availability, Maintainability & Safety.
2	EN 50128	Railway Applications-Communications, Signalling and processing systems-Software for Railway Control and Protection Systems.
3	EN 50129	Railway Applications-Communications, Signalling and processing systems- Safety Related Electronics Systems for Signalling.
4	EN50159-1	Railway Applications-Communications, Signalling and processing systems - Safety related communication in closed transmission systems.
5	EN50159-2	Railway Applications-Communications, Signalling and processing systems - Safety related communication in open transmission systems.
6	EN 50121-2/ IEC 62236-2	Railway applications – electromagnetic compatibility – Part 2: emission of the whole railway system to the outside world
7	RDSO/SPN/144	Safety and reliability requirement of electronic

		signalling equipment.
8	IRS: S 36	Relay Interlocking systems.
9	IRS: S 23	Electrical Signalling and Interlocking Equipment
10	RDSO/SPN/192	Electronic Interlocking
11	RDSO/SPN/147	Universal Fail-Safe Block Interface
12	IEEE 802.3, 802.3u, 802.3x, 802.1d, 802.1w, 802.1p, 802.1Q	IEEE Standard for Information technology-Specific requirements for Ethernet communication in managed switch

4 GENERAL REQUIREMENTS

4.1 The system and its accessories shall comply with the requirements of signalling circuits using electronic equipment as laid down in Signal Engineering Manual Part-I 1988 (Para 7.121 to 7.130) and as stipulated in RDSO/ SPN/ 144/2006.

4.2 The system shall comply with the specification no. RDSO/ SPN/ 144/2006 for safety and reliability requirements of Electronic Signalling equipment.

4.3 The system shall comply with the environmental/ climatic requirements as specified in RDSO/SPN/144/2006.

4.4 The system shall be capable of working in non-air-conditioned environment ambient varying from -10^{o}C to +70^{o}C.

4.5 The equipment shall be so constructed as to prevent unauthorized access to the system.

4.6 The system shall be fully tested to ensure that it is free of systemic errors at the time of commissioning.

4.7 Interface equipment shall be so designed that no modification, either technical or operational is required in the equipment, which are interfaced.

4.8 The termination of wires and housing rack shall be constructed to comply with requirements stipulated in RDSO/ SPN/ 144/2006.

4.9 Insertion of PCB in wrong card slots should not be possible.

4.10 Suitable lightning and surge protectors shall be provided as per RDSO/SPN/144/2006.

4.11 MTBF of the system shall be better than 50000 hours.

4.12 The equipment shall offer ergonomic ease in its operation and maintenance.

5 FUNCTIONAL REQUIREMENTS

A. NON-VITAL I/O MODULE

5.1 This module can be used for non vital functions requiring maximum safety integrity level 2, i.e., information exchange between panel and interlocking, display information from field (not for proving circuits).

5.2 The equipment shall be compatible with 24V DC signal driven systems like relays, indicating lamps etc. It shall be able to sense an Input by reading complementary potential free contacts (1NO + 1NC) from Q-series, metal-metal or miniature relays or metal switches used in panels.

5.3 The module shall be able to communicate over any reliable full duplex Dual 10/100 Mbps Ethernet bus or star network using Dual redundant copper cable/OFC / radio communication media.

5.4 The system shall work on 24V DC (+20%, - 20 %.)

5.5 The module errors will be logged in an on-board event logger module forlast 10,000 events. It shall be possible to see the logged errors by means of front panel display unit. Event logger should have a built in webserver that should be reachable over user defined IP address with secure access.

5.6 The system shall cater upto 256 I/O in blocks of 32 I/O. Each output port shall be capable of outputting 24V (23-25 V) / 100 ma (min.) to drive signalling relays. For the purpose of sensing inputs, potential free contacts of relays/switches shall be used. It shall be possible to commission the system with even a single 32 I/O module.

5.7 Each output should be individually short circuit protected and must be inherently capable of driving 3 times the rated load, to prevent damage during short circuit. Normal working should be resumed automatically after removal of the shorting.

5.8 The equipment shall be capable of working on full Duplex 10/100 Mbps Ethernet port provided cable/OFC / Microwave radio, simultaneously on redundant Ethernet ports with unique MAC addresses of minimum 32 bits.

5.9 In case of disruption of communication link between two locations or failure of the equipment, all the output must go low within a period of 3-5 seconds.

5.10 The pair of equipment shall be transparent to the signalling circuit / equipment connected through them.

5.11 Each mux module in the section shall have a 16- bit unique address, which shall be stored in the system. Address of the adjacent equipment shall be hard wired.

5.12 The information exchanged between the pair of the interface equipment shall contain the source & destination address.

B. <u>VITAL I/O MODULE</u>

5.13 This module shall have safety integrity level of 4 and will be used for vital signalling functions that can be used for proving, control and interlocking.

5.14 The equipment shall be compatible with 24V DC signal driven systems like relays, indicating lamps etc. It shall be able to sense an Input by reading complementary potential free contacts (1NO + 1NC) from Q-series, metal-metal or miniature relays.

5.15 The module shall be able to communicate over any reliable full duplex Dual bus or star network on cable/OFC / radio media. The communication network shall necessary be a Closed Network,

- Only approved access is permitted
- There is a maximum and known number of connectable participants
- Transmission should be known and fixed

5.16 The system shall work on 24V DC (+20%, - 20 %.)

5.17 The system must be having a 2 out of 3 or dual redundant 2 out of 2 architecture with hot swappable modules

5.18 The module errors will be logged in an on-board event logger module for last 10,000 events. It shall be possible to see the logged errors by means of front panel display unit. Event logger should have a built in webserver that should be reachable over user defined IP address with secure access..

5.19 The system shall cater upto 256 I/O in blocks of 8 I/O Each output port shall be capable of outputting 24V (+/- 1V) / 100 ma (min.) to drive signalling relays. For the purpose of sensing inputs, potential free contacts of relays shall be used. It shall be possible to commission the system with even minimum64 I/O module.

5.20 Each output should be unreferenced, individually short-circuit protected isolated DC-DC converter and must be inherently capable of driving 3 times the rated load, to prevent damage during short circuit. Normal working should be resumed automatically after removal of the shorting.

5.21 The equipment shall be capable of working on full Duplex port provided over cable/OFC / radio, simultaneously on redundant ports.

5.22 In case of disruption of communication link between two locations or failure of the equipment, all the output must go low in less than 3 seconds.

5.23 The pair of equipment shall be transparent to the signalling circuit / equipment connected through them.

5.24 Each module shall have a 16- bit unique address, which shall be stored in the system. Address of the adjacent equipment shall be hard wired.

5.25 The information exchanged between the pair of the interface equipment shall contain the source & destination address.

C: VITAL TRACKSIDE FUNCTION MODULE

5.26 This module is optional and intended for directly driving functions like signals, points etc by switching a power supply of 110 V AC/ 110V DC.

5.27 Signal aspect lit proving shall be inbuilt by the return current from aspect circuit.

5.28 The module errors will be logged in an on-board event logger module for last 10,000 events. It shall be possible to see the logged errors by means of front panel display unit. Event logger should have a built in webserver that should be reachable over user defined IP address with secure access

5.29 In case of disruption of communication link between two locations or failure of the equipment, all the output must go low in less than 3 seconds.

5.30 The pair of equipment shall be transparent to the signalling circuit / equipment connected through them.

5.31 Each module shall have a 16- bit unique address, which shall be stored in the system. Address of the adjacent equipment shall be hard wired.

6 NETWORK ARCHITECTURE

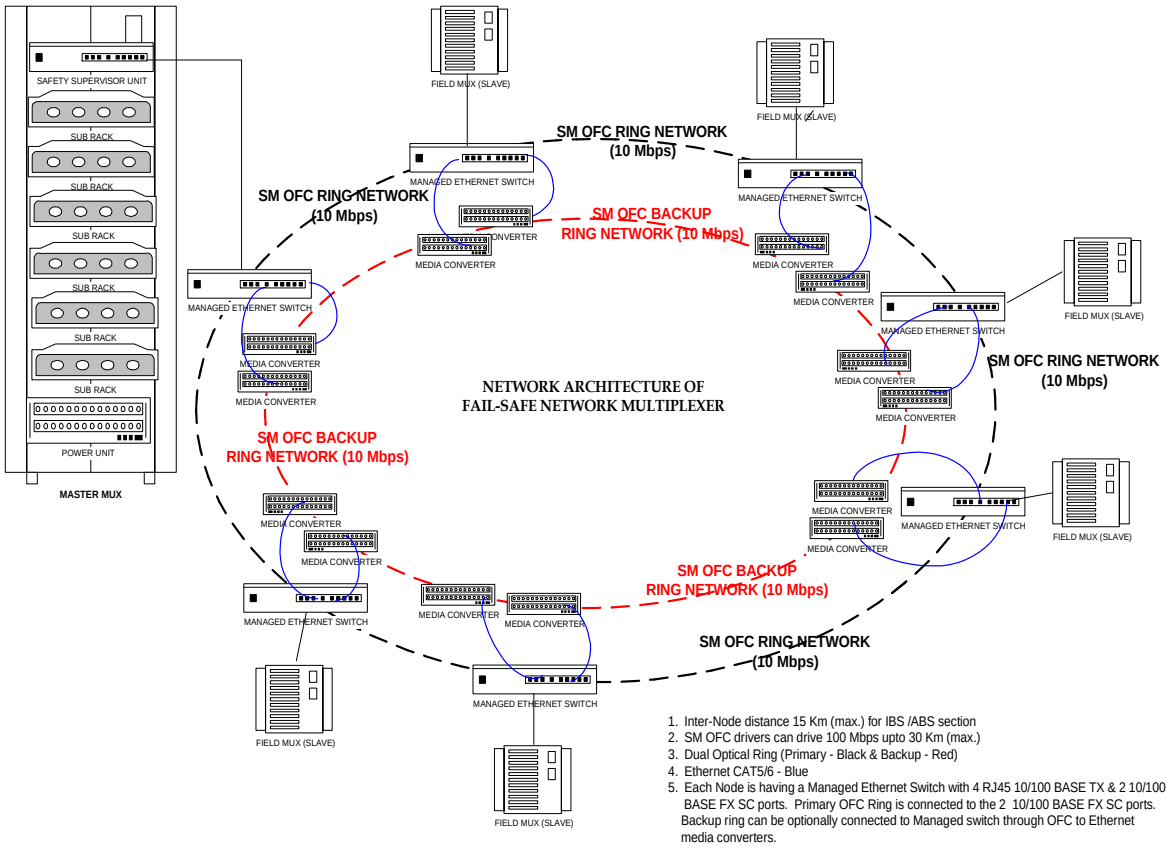
6.1 The system comprising of the Vital & Non-Vital module shall be capable to work on Dual Redundant OFC Ring Network with 10/100 Mbps Ethernet or any other suitable and proven protocol for safety systems. The network shall be composes of easily available and industry standard network components available across manufacturers.

6.2 The network elements shall be mutually interchangeable and compatible.

6.3 The network elements shall be capable of working in same electrical and climatic condition for temperature, shock, freefall and vibration (in compliance with RDSO/SPN/144/2006) as that of the I/O modules and must have MTBF better than 15 years.

6.4 Single Mode OFC shall be used for establishing the optical backbone

6.5 No special / proprietary protocol or encryption should be used in the network level, so that it shall be possible for an authorized user to add or delete a pair of modules.



7 SYSTEM ARCHITECTURE

a) The mux should have a centralized Master unit in at a station, while the slave units are placed in location boxes at the location boxes at the foot of the signal or point, in order to drive the unit and detect its proper operation.

b) The Master Mux shall be responsible for,

i. Collection of different field status (like the lamp proving relays, point detection relays and track relays), as required from the field and deliver the relevant information, into a centralized location.
ii. The Master Mux shall operate from low ripple 24V DC (-20% / +20%) axle counter battery charger or IPS module, All other voltages necessary for its internal operations will be derived from this voltage.
iii. The Master Mux shall have individual modules with unique 16 bit address and a defined set of preset IP Address / MAC ID, which will be appended with the data packets in order to ensure proper delivery at exact locations.
iv. There shall be individual modules / sub-racks to communicate with each slave units i.e. module 1 should only "talk" with slave mux 1 and module 2 should only "talk" with slave mux 2, and so on.
v. Each of theVital Fail-Safe (SIL-4) module / sub-racks in the Master Mux shall have 2 out of 3 OR dual 2 out of 2 Fail-Safe (SIL-4) Intelligent 8/16 Input –8/ 16 Output module, for delivering maximum availability.
vi. Each of theNon-Vital (SIL-2) module / sub-racks in the Master Mux may have hot standby I/O module, for delivering maximum availability, if deemed necessary for the application.
vii. The Master Mux may have dedicated hot standby power supply for driving both Vital Fail-Safe (SIL-4) & Non-Vital (SIL-2) Input / Output module
viii. Each of theVital Fail-Safe (SIL-4) modules in the Master Mux shall have scalability upto256 Input &256 Output. While Non-Vital (SIL 2) module may have upto 128 I/O capability in blocks of 32 I/O, by the use of a single CPU.
ix. An optional CPLD / FPGA based dedicated 2 out of 2 hardware logic unit for resolving the ABS / IBS /Point Drive & Sense logic unit will be coupled with every modules in the Master Mux.
x. The interconnection of the CPLD / FPGA based hardware logic unit to the module / sub-racks or between 2 consecutive module / sub-racks in the Master Mux, shall be through physical wire connection i.e. flat / ribbon / braided cable only, protecting against any wrong interconnection.
xi. All the input shall be complementary 1NO + 1 NC and outputs shall be mutually isolated 24V / 200 mA DC enough for driving 2 nos. Q-series relays, with read back for output integrity check.

c) The Slave Mux Unit shall be responsible for,

i. Sensing of different field status (like the lamp proving relays, point detection relays and track relays), as required from the field and deliver the relevant information, into a centralized location.
ii. The Slave Mux shall have individual modules with unique 16 bit address and a defined set of preset IP Address / MAC ID, which will be appended with the data packets in order to ensure proper delivery at module / sub-racks in the Master Mux.
iii. These Slave Mux shall be able to communicate with its target modules / sub-racks in Central location i.e. slave mux 1 should only "talk" with module 1 and slave mux 2 should only "talk" with module 2, and so on.
iv. The Slave Mux shall have a 2 out of 3 Fail-Safe (SIL-4) or dual 2 out of 2 working in parallel, for delivering maximum availability.
v. In case of theNon-Vital (SIL-2) Slave Mux module / sub-racks in the itmay be used in hot standby I/Oconfiguration, for delivering maximum availability, if deemed necessary for the application.

vi. Each of the Vital Fail-Safe (SIL 4) Slave Mux shall have dedicated hot standby power supply for each of the 2 out of 3 Fail-Safe (SIL-4) or dual 2 out of 2 working in parallel

vii. Each of theVital Fail-Safe (SIL-4) module in the Slave Mux shall have capability of 16 Input & 16 Output. While Non-Vital (SIL 2) module may have upto 128 I/O capability in blocks of 32 I/O, by the use of a single CPU.

viii. Non-Vital (SIL 2) module in Slave Mux shall be used for centralized collection of different field status for indication and data-logging purpose.

8 SYSTEM COMPOSTION

A. VITAL I/O MODULE

i. The Fail-Safe (SIL-4) Intelligent Input –Output module, shall inherit the basic Functional Requirement specification and the technical specifications of RDSO/SPN/147/2005. Except the fact that it shall be possible to work the system with 2 out of 2 CPU in Hot standby configuration, in the same hardware / software or different hardware / software.

ii. For transmission of safe relay state Ethernet based validated safety protocols like ProfiNet, TCP/IP, Ether CAT may be used in addition to serial communication platform (RS-232 / RS-422 / RS485), as stated in RDSO/SPN/147/2005.

iii. The communication media shall be primarily single / multi mode OFC. Suitable network devices and communication mux / modem / switch /router should be used. The communication interface can either be an onboard component or standard COTS unit with certified quality and MTBF and widely used in Railway industry.

iv. The Q -series (that were present in UFSBI for galvanically isolated I/O interfacing), shall be replaced by improved, efficient and miniaturized optically / galvanically isolated interfacing circuit to achieved desired level of I/O isolation (2 KV min.) and safety target (SIL-4).

v. The units should have an on-board event logging facility capable of storing last 10,000 error codes with time stamps.

B. NON-VITAL I/O MODULE

i. In order to maintain safety (SIL 2) the following hardware features shall be specifically adapted to the design of interface.

(a) Watch dog timer for checking the process, the processor and other device activities.

(b) Output latches with read back.

(c) Use of opto-isolators (min. 2 KV) for input isolation.

(d) Equipment addressing and fixed message length.

(e) In case any industry standard protocols like ProfiNet, CAN Open, UDP or TCP/IP is used the safety certified software components with suitable evidence should only be used.

(f) Conformal coating & metallic shielding of all cards for rough environments.

(g) Natural air-cooling.

(h) Use of either transformer or opto-isolators (min. 2 KV) for isolation of digital circuits and output relays.

(i) Outputs are read back for cross checking.

(j) The digital ICs used in the equipment shall be capable of withstanding surface temperature of 85^0C.

(k) The discrete components like diodes, transistors, SCRs etc. should comply with RDSO/SPN/144.

(l) All power supplies on cards where digital ICs are used shall be locally decoupled using capacitors of good high frequency characteristics.

(m) To protect against the electromagnetic interference, at least two of shielding should be provided i.e.

- Shielding at card level by providing a metallic plate over the cards.
- Shielding at chassis/ rack level.

ii. The system shall comprise of the following modules/ functions:

- Dual Redundant Power supply module
- PIC32 / ARM core 32-bit Processor and communication Modules
- Complementary Input sensing Modules
- Output Modules (for driving relay / indication)
- Chassis Backplane

C. POWER SUPPLY MODULE

i) The power supply module shall work with input voltage of 24 volt DC (-20% / +20%)

ii) The ripple voltage in the output shall not exceed 50 mv peak to peak for +5V supply at 40 MHz bandwidth. The output ripple voltage (peak to peak) of other than +5V output shall not be more than 1% of the rated output voltage at full load.

iii) Monitored hot standby module shall be provided for better reliability.

iv) Glass fuses of proper rating shall be provided to protect the equipment.

v) The power supply module shall have self re-setting type protection from under voltage of DC input, over voltage of DC input, over load of DC output & short circuit of DC output.

vi) Voltage regulation shall be less than 1% of output rated voltage.

D. CPU Module

This module shall be designed to facilitate following functions:

(a) Decoding of the incoming message and transmission of the relevant information to the corresponding output module.

(b) Receiving of the message from the input module, encoding the message telegram and communicating with communication controller module.

(c) Communication only with adjacent equipment that is having paired address with the unit.

(d) Controlling and allotting the dual communication ports each having unique MAC address.

E. Input Modules

Input module shall be so designed that two optical isolators sense back and front contacts of the relays / switches. After proper sensing of the complementary contacts, data is send to processor module.

F. Output modules

Message regarding status of the input is read from remote module through communication port is decoded and outputs are generated by the output driver circuit. Status of each output should be continuously monitored.

a. An integrated display system shall be provided for display of both local and far end faults.
b. Integrity of the output driver circuit should be checked periodically to guard against inadvertent energisation of the relays.

G. Integrated Failure Event Logger Module

At least last 10,000 events with time-stamp should be logged on the on-board memory of the CPU on FIFO basis. It shall be possible to extract the data from the Mux to a computer.

9 SAFETY REQUIREMENTS (FOR SIL-2 / SIL-4 MODULE)

8.1 The UFSBI shall assign specific addresses to each System (By Hard Wired Logic) and ensure that the message/ telegram sent is received by the System for which it is meant.

8.2 The coding of signal information shall take care of type of noise generally encountered in the transmission system and ensure safety in operation against those noise levels.

8.3 Codification of input data for transmission must ensure a hamming distance of 5 or better and at least 2 out of 3 consecutive message redundancy checks must be ensured.

8.4 In case of disruption of the communication link between two stations or failure of interface equipment, there shall be no out of correspondence in indications at the two stations with regard to the position of the I/O's . In link failure condition needle should go back to the line closed.

8.5 The information exchanged between the pair of the interface equipment shall contain all safety-related data e.g. (Sync1, source address, destination address, Data, inverted data, Redundancy Bytes etc.).

8.6 Wrongly addressed information packets shall be promptly rejected by the system and continuous receipt of such packets should raise an alarm and result in shutdown of the system.

8.7 With respect to the inputs the following requirements shall be satisfied:

(a) Proper debouncing technique should be adopted for the input reading process.
(b) Inputs must be isolated by opto-isolators and separate opto-isolators must be used for the same input in order to provide multiple signal paths for multiple processing of input data.

8.8 With respect to the outputs the following requirements shall be satisfied:

(a) Data written to the individual output latches must be read back through the processor bus for integrity. In case of mismatch, the system processes a restrictive mode.
(b) Presence of any other unwanted signal should not lead to unsafe conditions.

8.9 In the event of a failure of any component/ module/ sub-system or bug in the software, the system shall put that output to the most restrictive mode of operation and remove power from the physical output in a fail-safe manner, till fault removed. An error with suitable error code will be logged.

8.10 Unsafe condition shall not develop due to faults and adequate safety margins must be incorporated in the design for all modes of failure for the following:

(a) High impedance and open circuit fault of a component and multi-terminal devices.
(b) Low impedance and short circuit faults of a component and multi-terminal device.
(c) Variation in the component values beyond their tolerable limits.
(d) Operational faults likely to lead to unsafe condition.
(e) "Stuck at Faults" particularly in comparator circuits, I/O circuits, controlling circuits of microprocessor etc.
(f) Fleeting errors in memory chips data buses, if any.
(g) Damages to the data bus.

8.11 No single failure shall result in an un-intended output condition. The failure should be suitably indicated and must be logged.

8.12 The design of the equipment shall cater for detection and restoration of system to a safer state in case of following faults if these are likely to result in un-intended output condition:

(a) Variation in power supply beyond its tolerance limits, including momentary failure of the power supply module.
(b) Spikes in the power supply system, stray fields caused by traction vehicles or standby diesel generator sets.
(c) Earthing of any component or wire or a combination of such earthing faults.
(d) Broken wires, damaged or dirty contacts, failure of a component to energies, loss of power supply or blown fuses etc.

8.13 System should comply with SIL-2 of CENELEC standard or equivalent standard.

9 TRANSMISSION OF SAFETY INFORMATION

9.1 In the systems requiring transmission of vital safety information, the following requirements shall be fulfilled:

I. It shall be possible to transmit the safety information over Ethernet channels through telecom cable as well as through any media using proper multiplexers / media converters. The communication protocol should ensure integrity of safety related information irrespective of the transmission medium.

II. If communication fails for a short duration i.e. upto three frames then the last valid output data shall be held. If communication failure is for a longer duration i.e. more than three seconds, the system shall assume most restrictive and safe state.

III. Errors introduced or not detected at a given level in the transmission system must be detected at higher levels. Error detection methods used at any level must take into account the characteristics of the lower levels.

IV. Error detection techniques should permit the use of standard telecommunication techniques, which offers much more economic solution than the special hardware needed to implement error prevention techniques.

V. Error detecting coding shall not form the sole means of protection of transmitted information, but should be combined with other methods such as higher level procedures and protocols.

VI. Forward error correcting coding shall not be used.

VII. The response time should be less than 400 msec. for the complete system up to a Ethernet on OFC or microwave radio. Communication drivers should be able to provide necessary bandwidth on the working media.

10 SOFTWARE AND VALIDATION

10.1 Software used in Mux systems should have been developed in conformity with a software engineering standard issued by recognized standards body such as European Committee for Electro Technical Standardization (CENELEC) with special relevance to SIL-2 / SIL-4, as applicable for the Non-Vital and Vital modules respectively.

10.2 The software shall conform to all the safety requirements of signalling operation. Design shall ensure that during malfunction of the Mux the specific output will be inhibited and the nature of fault should be logged.

10.3 The software shall be developed in such a way that it is possible to test and validate each module independently.

10.4 The software shall be such that in case of variable data, the possibility of using incorrect data does not exist. Further the software should check and reject:

(a) Use of data which is obsolete or meant for some earlier state of the system, and
(b) Corrupted data.

10.5 As far as possible, program flow shall be independent of the input data. The program should preferably execute the same sequence of instructions in each cycle.

10.6 The use of hardware interrupts shall be kept to a bare minimum.

10.7 Software should include self-check procedures to detect faults in the hardware, memory, stack communication / backplane bus etc.

10.8 Self-check of the associated functional hardware as required by the hardware design should be performed periodically.

10.9 The following shall ensure:

a) Error detection capability of data packets
b) 2 out of 3 message redundancy
c) Correspondence check between inverted and non-inverted signals.

10.10 As specified in the software Engineering Standards, full documentation on Quality Assurance Program specially the Verification and Validation (V&V) procedures carried out in-house or by any independent agency should be made available to RDSO to check their conformity to standards. If the procedure and documentation for V&V is considered inadequate, RDSO reserves the right to get the verification and validation of software and hardware done by an independent agency at the cost of the supplier.

11 MAINTENANCE, TESTING AND DIAGNOSTIC REQUIREMENTS

11.1 To ensure that the above safety criteria is maintained, the system shall have diagnostic checks carried out at frequent intervals, monitoring a condition giving appropriate indications and alarms.

11.2 The system shall be provided with a front-panel alphanumeric LCD display unit indicating various failures. The error code should indicate the type of the failure.

11.3 A trouble-shooting chart should be provided indicating the action required to be taken for repair of the equipment corresponding to each error code.

11.4 Audio visual alarm shall be provided in case of failure. The audio alarm should stop when acknowledged but the visual alarm should be logged.

11.5 Necessary provision shall be made in the hardware and software for modular expansion of the equipment.
