DRAFT SPECIFICATION FOR
Failsafe Networked Multiplexer (FNmux)

Specification No.- RDSO/SPN/211/2019
Version - 1.0 (d4) (Draft)
## DOCUMENT DATA SHEET

<table>
<thead>
<tr>
<th>Designation</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDSO/SPN/211/2019</td>
<td>1.0(d4)(Draft)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title of Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft Specification for Failsafe Networked Multiplexer (FNmux)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authors:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Shri Hari Om Kushwaha</td>
</tr>
<tr>
<td>Designation: Director/Signal-VI, RDSO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Shri Sandeep Mathur</td>
</tr>
<tr>
<td>Designation: ED/Signal Co-ordination, RDSO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abstract:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This document defines draft specification for Failsafe Networked Multiplexer (FNmux)</td>
</tr>
</tbody>
</table>
### DOCUMENT CONTROL SHEET

<table>
<thead>
<tr>
<th>NAME</th>
<th>ORGANISATION</th>
<th>FUNCTION</th>
<th>LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pradeep Saxena</td>
<td>RDSO</td>
<td>Member</td>
<td>Prepare</td>
</tr>
<tr>
<td>Hari Om Kushwaha</td>
<td>RDSO</td>
<td>Member</td>
<td>Checking</td>
</tr>
<tr>
<td>Anurag Goyal</td>
<td>RDSO</td>
<td>Checking Authority</td>
<td>Review</td>
</tr>
<tr>
<td>Sandeep Mathur</td>
<td>RDSO</td>
<td>Approving Authority</td>
<td>Approve</td>
</tr>
</tbody>
</table>
### AMENDMENTS:

<table>
<thead>
<tr>
<th>Specification No.</th>
<th>Version</th>
<th>Amendment</th>
<th>Amendment Details</th>
<th>Effective date</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDSO/SPN/211/2012</td>
<td>0.1</td>
<td>-</td>
<td>Draft</td>
<td>-</td>
</tr>
<tr>
<td>RDSO/SPN/211/2014</td>
<td>0.2</td>
<td>first</td>
<td>Updating with comments from EOI participants</td>
<td>December 2014</td>
</tr>
<tr>
<td>RDSO/SPN/211/2017</td>
<td>1.0 d3</td>
<td>Draft</td>
<td>Updating requirements of Commercially of the self (COTS) SIL 4 equivalent products and vigilance directive</td>
<td>17.10.2017</td>
</tr>
<tr>
<td>RDSO/SPN/211/2019</td>
<td>1.0 d4</td>
<td>Draft</td>
<td>Updating with comments from Zonal Railways, Firms and one more indigenous vendor of M/s TSTS, Bangalore</td>
<td>DD.MM.2019</td>
</tr>
</tbody>
</table>
Table of Content

<table>
<thead>
<tr>
<th>SN</th>
<th>Chapter</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.</td>
<td>Foreword</td>
<td>6</td>
</tr>
<tr>
<td>1.</td>
<td>Scope</td>
<td>6</td>
</tr>
<tr>
<td>2.</td>
<td>Terminology</td>
<td>6</td>
</tr>
<tr>
<td>3.</td>
<td>Applicable documents</td>
<td>7</td>
</tr>
<tr>
<td>4.</td>
<td>General Requirements</td>
<td>7</td>
</tr>
<tr>
<td>5.</td>
<td>Functional Requirements</td>
<td>8</td>
</tr>
<tr>
<td>6.</td>
<td>Fail safety Requirements</td>
<td>12</td>
</tr>
<tr>
<td>7.</td>
<td>Transmission of safety information</td>
<td>14</td>
</tr>
<tr>
<td>8.</td>
<td>Software and validation</td>
<td>15</td>
</tr>
<tr>
<td>9.</td>
<td>Maintenance, Testing &amp; Diagnostic requirements</td>
<td>17</td>
</tr>
<tr>
<td>10.</td>
<td>Tests &amp; Requirements</td>
<td>17</td>
</tr>
<tr>
<td>11.</td>
<td>Quality Assurance</td>
<td>19</td>
</tr>
<tr>
<td>12.</td>
<td>Plant &amp; Machinery</td>
<td>19</td>
</tr>
<tr>
<td>13.</td>
<td>Packing</td>
<td>20</td>
</tr>
<tr>
<td>14.</td>
<td>Information to be supplied by the Manufacturer</td>
<td>20</td>
</tr>
<tr>
<td>15.</td>
<td>Options to be specified by the purchaser</td>
<td>20</td>
</tr>
<tr>
<td>16.</td>
<td>Block Working Diagram of FNmux(CU) to FNmux(FU)</td>
<td>21</td>
</tr>
<tr>
<td>17.</td>
<td>Block Working Diagram of FNmux(FU) to FNmux(FU)</td>
<td>22</td>
</tr>
</tbody>
</table>
0 **FOREWORD**

0.1 This specification is issued under the fixed serial number RDSO/SPN/211 followed by the year of adoption as standard or in case of revision, the year of latest revision.

0.2 Whenever, reference to any specification appears in this document, it shall be taken as a reference to the latest version of that specification unless the year of issue of the specification is specifically stated.

1 **SCOPE**

1.1 This specification covers the technical and operational requirements of the Fail-Safe Network Mux for exchanging vital signaling information using Dual redundant OFC / reliable wireless communication media in a fail-safe (SIL-4) manner.

2 **TERMINOLOGY**

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

2.2 **ABBREVIATIONS:**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FNmux</td>
<td>Fail-Safe Networked Multiplexer</td>
</tr>
<tr>
<td>UFSBI</td>
<td>Universal Fail-Safe Block Interface</td>
</tr>
<tr>
<td>FNmux(CU)</td>
<td>FNmux (Central Unit)</td>
</tr>
<tr>
<td>FNmux(FU)</td>
<td>FNmux (Field Unit)</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean time between Failure</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time to Failure</td>
</tr>
<tr>
<td>MTBWSF</td>
<td>Mean Time between Wrong Side Failures</td>
</tr>
<tr>
<td>CENELEC</td>
<td>European Committee for Electrotechnical Standardization</td>
</tr>
<tr>
<td>EN</td>
<td>European Standards</td>
</tr>
<tr>
<td>IEEE-SA</td>
<td>Institute of Electrical and Electronics Engineers Standards Association</td>
</tr>
<tr>
<td>IEEE 802.3</td>
<td>IEEE 802.3 specifies the physical and networking characteristics of an Ethernet network, like how physical connections between nodes</td>
</tr>
</tbody>
</table>
(routers/switches/hubs) are made through various wired media like copper coaxial or fiber cable.

2.2.12 SIL- 4 Safety integrity level - 4
2.2.13 EMF Electro-Motive force

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Subject</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EN50126</td>
<td>Railway Application Specifications and Demonstration of Reliability, Availability, Maintainability &amp; Safety</td>
</tr>
<tr>
<td>2</td>
<td>EN 50128</td>
<td>Railway Applications-Communications, Signaling and processing systems-Software for Railway Control and Protection Systems.</td>
</tr>
<tr>
<td>3</td>
<td>EN 50129</td>
<td>Railway Applications-Communications, Signaling and processing systems- Safety Related Electronics Systems for Signaling.</td>
</tr>
<tr>
<td>4</td>
<td>EN50159</td>
<td>Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems.</td>
</tr>
<tr>
<td>5</td>
<td>EN 50121-2</td>
<td>Railway applications – electromagnetic</td>
</tr>
<tr>
<td>6</td>
<td>IEC 62236-2</td>
<td>Compatibility – Part 2: emission of the whole railway system to the outside world</td>
</tr>
<tr>
<td>7</td>
<td>RDSO/SPN/144</td>
<td>Safety and reliability requirement of electronic signaling equipment.</td>
</tr>
<tr>
<td>8</td>
<td>IRS: S 36</td>
<td>Relay Interlocking systems</td>
</tr>
<tr>
<td>9</td>
<td>IRS: S 23</td>
<td>Electrical Signaling and Interlocking Equipment</td>
</tr>
<tr>
<td>10</td>
<td>RDSO/SPN/192</td>
<td>Electronic Interlocking</td>
</tr>
<tr>
<td>11</td>
<td>IRS:S-104/2012</td>
<td>Universal Fail-Safe Block Interface</td>
</tr>
<tr>
<td>12</td>
<td>IEEE 802.3, 802.3u, 802.3x, 802.1d, 802.1w, 802.1p</td>
<td>IEEE Standard for Information technology-Specific requirements for Ethernet communication in managed switch</td>
</tr>
</tbody>
</table>

3. APPLICABLE DOCUMENTS

4. GENERAL REQUIREMENTS

4.1 The system and its accessories shall comply with the requirements of signaling 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 (latest).

4.2 The system shall comply with the specification No.-RDSO/SPN/144/2006/latest for safety, reliability and Environmental/Climatic requirements of Electronic Signaling equipment.
4.3 The system shall be capable of working in non-air-conditioned environment ambient temperature varying from -10°C to +70°C. The system shall be able to be used in indoor/outdoor environment.

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

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

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

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

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

4.9 Suitable lightning and surge protectors shall be provided as per RDSO/SPN/144/2006 (latest).

4.10 MTBF of the individual equipment shall be better than 100000 hours.

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

5. FUNCTIONAL REQUIREMENTS

Failsafe Network Multiplexer system will consist of distributed multiplexer modules, connected in a network, constituting a network of fail-safe multiplexer modules for exchange of vital digital I/O information. The system architecture shall allow the formation of a scalable centralized Unit of modules (FNmux Central Unit or CU) to concentrate I/O from the distributed field modules (FNmux Field Unit or FU). Furthermore, the network protocol and addressing technique adopted shall be such that any pair of vital modules, either in the Central Unit or in the Field Unit can be virtually connected from any point to any point.

a) **FNmux Central Unit (CU):** The Central Unit will consist of a variable number of vital modules. Central Unit shall have CENELEC SIL-4 compliant fail-safe **2oo2 or 2oo3 architecture** in hot standby mode. Other modules of the central unit shall have CENELEC SIL-4 compliant fail-safe architecture configuration with at least 64 digital I/O for transferring of vital point, signal, tracks and other similar vital relay status. The CU should be modular in nature and expandable upto minimum 256 digital I/Os. The Transfer to hot standby system should be seamless, without affecting safety & ongoing operations.

b) **FNmux Field Unit or (FU):** Each module shall have CENELEC SIL-4 compliant fail-safe architecture, configuration with at least 64 digital I/O (in same chassis / box size of 3U/42T OR (comparable/similar) dimensionally suitable to be installed in field location box for transferring of vital point, signal, tracks and other similar vital relay status. FNmux Field Unit shall be able to transfer vital information to CU
and among themselves, independent of CU.

c) Communication architecture shall comprise of dual redundant single mode OFC (AS PER IRS/TC/55/2006 OR LATEST) Ring network, suitable for Ethernet traffic up to distance of 30 Kms at 10/100/1000 Mbps.

d) It shall be having diagnostic features for monitoring the health of the system.

5.1 **FNmux CENTRAL UNIT (CU)**

5.1.1 FNmux Central Unit shall have Safety Integrity Level of 4 (SIL 4) and will be used for transferring vital signaling information and for performing certain vital signaling functions.

5.1.2 It shall have Fail-safe 2oo2 or 2oo3 architecture in hot stand by mode.

5.1.3 The equipment shall be compatible with 24V DC (-20% to +30%) signal driven systems like relays, indicating lamps etc.

5.1.4 The module shall be able to communicate over any reliable full duplex dual ring Ethernet network on OFC / reliable wireless communication media. The communication network shall necessary be a Closed Network with the following properties:
  - Only approved access is permitted
  - There is a maximum and known number of connectable participants
  - Transmission properties should be known and fixed.

5.1.5 The system shall work on 24V DC (-20% to +30%) or 110V, 50Hz (-20% to +30%) as specified by the purchaser.

5.1.6 The Central Unit shall cater minimum 64 I/O & shall be scalable upto minimum 256 I/Os by addition of modules. Each output port shall be capable to drive signalling relays using external or internal power supply, for the purpose of sensing inputs, potential free contacts of relays shall be used.

5.1.7 It shall be capable to interface with another CU and multiple FUs (Minimum 4 in Number) for exchanging signaling information.

5.1.8 Each output/Input shall have suitable protection for back E.M.F./Short ckt /Overload etc.

5.1.9 The equipment shall be capable of working on full Duplex Ethernet port provided over OFC / radio, simultaneously on redundant ports. Best quality gold plated RJ45 connector with LED indication type reliable Ethernet port or FX port must be provided.

5.1.10 In case of disruption of communication link between two nodes or failure of the equipment, all the output of the affected nodes or equipment must go low in not more than 3 seconds.

5.1.11 The pair of equipment shall be transparent to the signaling circuit / equipment connected through them.
5.1.12 Each module shall have a unique address, which shall be stored in the system. Address of the equipment shall be either hardwired or unique ID.

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

5.1.14 The CU shall be self-diagnostic system and shall be capable of interfacing with maintenance terminal or any PC to fetch the required information.

5.2 FNmux-(Field Unit):

5.2.1 This system shall have Safety Integrity Level of 4 (SIL 4) and will be used for transferring vital signaling functions with another FU or CU that can be utilized at required location.

5.2.2 It shall be capable to interface with one CU and Minimum Two FUs.

5.2.3 The equipment shall be compatible with 24V / 60V DC signal driven systems like relays, indicating lamps etc.

5.2.4 The module shall be able to communicate over any reliable full duplex single / dual ring network using safe Ethernet Protocol on OFC / reliable wireless media. The module shall be suitable to be used in a closed communication network with the following properties:

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

5.2.5 The system shall work on 24V DC (+30%, - 20 %.) or 110V, 50Hz (30%, - 20 %.) as specified by the purchaser.

5.2.6 Field Unit (FU) shall have CENELEC SIL-4 compliant fail-safe architecture. Each FU shall have at least 64I/Os using single or scalable modules. Each output port shall be capable to drive signaling relays using external or internal power supply for the purpose of sensing inputs, potential free contacts of relays shall be used.

5.2.7 Each output/Input shall have suitable protection for back E.M.F./Short ckt /Overload etc.

5.2.8 The equipment shall be capable of working on full Duplex Ethernet port provided over OFC / reliable wireless media simultaneously on redundant ports. Best quality gold plated RJ45 connector with LED indication or reliable Ethernet port or FX port must be provided in each Vital I/O modules in CU or FU.

5.2.9 In case of disruption of communication link between two locations (Nodes) or failure of the equipment, all the output of the affected peers or equipment must go to fail-safe state without affecting the availability of system adversely.

5.2.10 Each module shall have a unique address, which shall be stored in the system. Address of the equipment shall be either hardwired or
unique ID.

5.2.11 The information exchanged between the Nodes (field to central or field to field) of the interface equipment shall contain the source & destination address.

5.3 OTHER REQUIREMENTS:-

5.3.1 The modules shall be designed to facilitate following functions:

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

(b) Receiving of the message from the relay-input module, encoding the message telegram and communicating with other module.

5.3.2 RELAY INPUT MODULES

Relay input module shall be so designed that it senses the relay contacts (front contacts in case of metal to carbon relay, and both front and back in case of metal to metal). The relay input module shall be capable to be isolated, double break input with the facility of double cutting.

5.3.3 RELAY OUTPUT MODULES

Relay output modules shall be capable of driving the output relay using Internal/external power supply with suitable protection. The Relay output module shall drive isolated output.

5.4 NETWORK ARCHITECTURE

5.4.1 The FNmux shall be capable to work on dual Redundant OFC Ring Network using Managed Layer 2 Ethernet switch with applicable protocol, with 10/100/1000 Mbps Ethernet or any other suitable and proven protocol for safety systems. Schematic block diagram is given in figure-1 & 2.

The Central Unit (CU) or the Field Unit (FU) having –

a) The network elements shall be mutually interchangeable and compatible across manufacturers. It should comply with deterministic nature & Class of service as specified by IEEE 802.1p.

b) Wide Temperature operation: -10 °C to +70 °C.

c) All the network elements used with the system shall be compliant to EN-50159.

5.4.2 The network elements shall be capable of working in same electrical and climatic condition for temperature, shock, free-fall and vibration (in compliance with RDSO/SPN/144/2006 (Latest.) as that of the I/O
modules and shall have similar MTBF.

5.4.3 It shall be possible for an authorized user having necessary permissions / password to add or delete a pair of modules.

5.5 POWER SUPPLY MODULE

5.5.1 The power supply module shall work with input voltage of 24V DC / 110 V DC / 110 VAC as specified in with following stipulation;

(i) The ripple voltage in the output shall not exceed 40 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.

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

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

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

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

(vi) Class-C & Class-D Surge Protection Devices for power line from reputed makes like OBO, Phoenix, DHEN or similar or any other RDSO recommended makes must be adopted.

(vii) The complete FNmux system FU and that of CU shall be connected to the existing earthing system of other signaling equipments.

6 FAIL-SAFETY REQUIREMENTS

6.1 The FNmux shall assign specific addresses to each Instrument/ System (By unique ID) and ensure that the message/ telegram sent is received by the FNmux module for which it is meant.

6.2 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.

6.3 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 or shall be compliant to CENELEC requirements of SIL-4 safety standard.
6.4. 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.) or shall be compliant to CENELEC requirements of SIL-4 safety standard.

6.5. 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.

6.6. The system shall be so designed to prevent unauthorized access. System shall shutdown in case of unauthorized interference/ forced pick up of relay.

6.7. With respect to the inputs the following requirements shall be satisfied:
   (a) Proper de-bouncing technique should be adopted for the input reading process. It shall be possible to have sensing either through constant 24 VDC / 60 VDC or Coded Test Pulses generated from the system itself, that ensures that only the particular Input is present and avoids any stray feed or Input electronics short-circuits.
   (b) Inputs must be isolated and duly protected.
   (c) for relay inputs, it shall be capable to provide double cutting arrangement.

6.8. With respect to the outputs the following requirements shall be satisfied:
   (a) Before writing the output or setting the output latches, the processor must exchange the output set (i.e. data received from far-end FNmux field / central unit) between them and in case of equality only, the processor shall process to output the data.
   (b) Presence of any other unwanted signal should not lead to unsafe Conditions.
   (c) For relay output, it shall be isolated output driving the relay.

6.9. In the event of a failure of any component/ module/ sub-system or bug in the software, the system shall revert all its vital output to the most restrictive mode of operation and remove power from the physical output in a fail-safe manner.

6.10. 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.
(g) Damages to the data bus.
(h) Back E.M.F. in case of outputs.

6.11. No single failure shall result in an unsafe condition i.e. the system shall be brought to a safe state as soon as failure occurs. The failure should be suitably indicated.

6.12. It must be ensured that if a failure of equipment occurs which by itself does not result in unsafe condition, but which in combination with a second or subsequent failure could result in an unsafe condition, then the first failure should be detected and negated. The probability of occurrence of a second failure, while the first failure has not been detected and negated should be negligible so that MTBWSF is compliant to SIL-4 of CENELEC Standard.

6.13. 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 unsafe 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.

6.14. System should comply with SIL-4 of CENELEC standard or equivalent Standard.

7.0. TRANSMISSION OF SAFETY INFORMATION

7.1. 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 communication backbone provided over redundant optic fiber cable through any media using industrial grade Layer-2 Ethernet switches. The transmission protocol should ensure integrity of safety related information irrespective of the transmission medium.

(ii) If communication fails then the last valid output data shall be held for safe duration as mentioned in safety case. For communication failure longer than that duration then the system shall assume most restrictive and fail-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 techniques of safe communication, 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, and hardware redundancy or diversity.

(vi) Forward error correcting coding shall not be used unless precautions are taken at the higher level to prevent invalid corrections from being accepted at the higher level.

(vii) The response time of the system should be adequate for the complete system (10/100 Mbps safe Ethernet backbone).

(viii) Class D Surge Protection Devices for data line from reputed makes like OBO, Phoenix, DHEN or similar or any other RDSO recommended makes must be adopted.

(ix) All communication and transmission of vital information should be compliant to CENELEC EN-50159 standard & media-independent.

8.0. SOFTWARE AND VALIDATION:

8.1. Software used in FNmux 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 safety critical applications. Particular software engineering standards used shall be specified and one complete set of such standards shall be made available to RDSO.

The software shall conform to all the safety requirements of block-operation. Design shall ensure that during malfunction of the FNmux, not only power is removed from the output circuits in a fail-safe manner but also the processors are prevented from executing codes at random.

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

8.3 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.
8.4 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.

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

8.6 Software should include self-check procedures to detect faults in the hardware. The self-check should include the following:

(a) Memory containing the vital software and data shall be checked periodically so that probability of corrupted software jeopardizing the safety of the equipment is minimized.

(b) Components of the CPU such as general purpose registers, program counters, stack pointers, instruction register, instruction decoder ALU etc. shall be checked periodically as far as practicable.

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

8.8 Critical and non-critical software should be segregated in the memory area so that special procedures to check the program flow may be adopted during the self-check process for the critical software.

8.9 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.

8.10 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. The agency selected must have previous experience of validating SIL-4 items for RDSO and must be approved by the Project Director, before assigning the validation work.

8.11 The software must check that

a) Inputs to the processors are correct
b) Program has been executed correctly
c) Data tables have not changed
d) Inputs and variable data are correct
e) No program segments have been skipped
f) The outputs are correct
g) The outputs have not been changed by device failure in an unsafe manner
h) Integrity of whole system (self-check)
9. MAINTENANCE, TESTING AND DIAGNOSTIC REQUIREMENTS:

9.1. 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.

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

9.3. Audio-visual alarm shall be provided in case of failure. The audio alarm should stop when acknowledged but the visual alarm should continue till the fault is rectified.

9.4. A system-reset switch be provided for starting the system operation and an electro-mechanical counter should be provided which should be incremented every time a reset operation is performed. System reset switch should have a sealing arrangement to prevent unauthorized operation.

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

10. TESTS AND REQUIREMENTS

10.1 Condition of Tests:

Unless otherwise specified all the tests shall be carried out at ambient atmospheric conditions.

10.2 For inspection of material, relevant clauses of IRS: S 23 and RDSO/SPN/144(Latest).Shall apply.

10.3 Test Equipment

Test equipments should be provided as per STR for Electronic Signaling equipment and should include the following:

i) Dual beam oscilloscope of 20 MHz bandwidth
ii) Digital multimeters – 3.1/2 digit display with facility of diode & transistor testing
iii) Frequency counter
iv) DC power supply (± 5V, 24V)
v) EPROM Programmer and UV eraser
vi) Megger (500V)
vii) LCR meter
viii) HV tester
ix) Function Generation
x) Digital IC tests
10.4 **Type Tests**

The following tests shall constitute type tests:

a) Visual inspection as per Clause 10.7
b) Insulation Resistance tests as per Clause 10.8
c) Card-level functional and fail-safety tests on all the cards
d) System-level functional and fail-safety tests
e) Environmental/climatic tests as per relevant clause of RDSO/SPN/144

[FNmux Central Unit (CU) & FNmux Field Unit (FU) shall be tested as outdoor Equipment].

f) Applied high voltage test as per clause 10.9.

Only a single FNmux Central Unit (CU) and a single FNmux Field Unit (FU) shall be tested for this purpose. The equipment shall successfully pass all the type tests for proving conformity with this specification. If the equipment fails in any of the type tests, the purchaser or his nominee at his discretion, may call for another equipment/card(s) of the same type and subject it to all tests or to the test(s) in which failure occurred. No failure shall be permitted in the repeat test(s).

10.5 **Acceptance Tests**

The following shall comprise acceptance tests:

a) Visual inspection as per Clause 10.7
b) Insulation Resistance tests as per Clause 10.8
c) Card-level functional tests on one card of each type
d) System-level functional and fail-safety tests

10.6 **Routine Tests**

The following shall comprise the routine tests and shall be conducted by manufacturer on every equipment and the test results shall be submitted to the inspection authority before inspection.

a) Visual inspection as per Clause 10.7
b) Insulation Resistance tests as per Clause 10.8
c) Card-level functional test on all the cards
d) System-level functional and fail-safety tests
e) Environmental stress screening test for PCB & sub-systems as per relevant clause of RDSO/SPN/144 (Latest).

10.7 **Visual Inspection**

The equipment shall be visually inspected to ensure compliance with the requirement of Clauses of this specification. The visual inspection will broadly include:

(i) **System Level Checking:**
   - Constructional details
   - Dimensional check
   - General workmanship
- Configuration

(ii) **Card Level Checking**
- PCB laminate thickness
- General track layout
- Quality of soldering and component mounting
- Conformal coating & shielding
- Legend printing
- Green masking

(iii) **Module Level Checking**
- Mechanical polarization
- General shielding arrangement of individual cards
- Indications and displays
- Mounting and clamping of connectors
- Proper housing of cards

10.8 **Insulation Resistance Test**

Insulation Resistance test shall be carried out as per relevant clause of RDSO/SPN/144/2006 (Latest).

10.9 **Applied High Voltage Test**

Applied High Voltage Test shall be carried out as per relevant clause of RDSO/SPN/144/2006 (Latest).

11. **QUALITY ASSURANCE**

11.1 All materials shall be of the best quality and the workmanship shall be of the highest class as per QAP standards laid down by RDSO.

11.2 The equipment shall be manufactured as per quality assurance procedure laid down so as to meet the requirement of the specification.

11.3 Amongst other requirements of the specification, validation and system of monitoring of QA procedure shall form a part of type approval. The necessary Plant, Machinery and Test Instruments as given below shall be available with the manufacturer.

12. **PLANT & MACHINERY**

Test equipments should be provided as per STR for Electronic equipment and should include the following:

i) Wave soldering station
ii) Burn in chamber
iii) Dry heat and Humidity chambers
iv) Cold chamber
v) PCB assembling zig
vi) Anti-static assembly
vii) EPROM/Micro-controller Programmer
viii) UV Eraser
ix) Microprocessor development system for the CPU / MCU used
x) Computer aided design system
12.1 **Test Instruments:**

All test instruments as given in Clause 10.3 shall be available with the manufacturer. Along with the prototype sample for type test, the manufacturer shall submit the Quality Assurance Manual, Operation, Maintenance & Fault Repairing Manuals.

13. **PACKING**

As per relevant clause of RDSO/SPN/144/2006 (Latest).

14. **INFORMATION TO BE SUPPLIED BY THE MANUFACTURER**

14.1 Documentation as per relevant clause of RDSO/SPN/144/2006 (Latest).

14.2 The manufacturer should supply the following information:

a) Design approach for the system;
b) Functions achieved in hardware & software;
c) Mode of interaction between hardware & software;
d) Salient features through which fail safety has been achieved e.g. use of a watchdog timer, automatic shutdown etc. &
e) Proof of safety.

15. **OPTIONS TO BE SPECIFIED BY THE PURCHASER**

a) Medium on which FNmux is intended to work single/dual OFC.
b) Depending on the inter nodal distance, the type of OFC cable (Single / Multi mode) used.
c) Whether there shall be Dual Redundant OFC ring through diverse routes or only a single ring.
d) The number of FNmux Central Unit (CU) and the number of FNmux Field Unit (FU) to be deployed.

#########################
Figure-1

Block Working Diagram of CU with FU
Block Working Diagram of FU with FU at Yard

Figure-2