RESEARCH DESIGNS & STANDARDS ORGANISATION
MANAK NAGER, LUCKNOW – 226 011

सत्यमेव जयते

SPECIFICATION FOR
Failsafe Network Multiplexer (FNmux)

Specification No.- RDSO/SPN/211/2022
Version: 1.0

DOCUMENT DATA SHEET		
Designation: RDSO/SPN/211/2022		Version-1.0
Title of Document: Specification for Failsafe Network Multiplexer (FNmux)		
Authors: Name: Shri Avadhesh Kumar Yadav Designation: Director/Signal- III/RDSO		
Approved By: Name: Shri Rajendra Dhambel Designation: Principal ED/S&T/RDSO		
Abstract: This document defines Specification for Failsafe Network Multiplexer (FNmux)		

DOCUMENT CONTROL SHEET

NAME	ORGANISATION	FUNCTION	LEVEL
Manoj Verma SSE/D/TELE	RDSO	Member	Prepare
S.K.Srivastava ADE/Sig-V	RDSO	Member	Checking
Avadhesh Kumar Yadav Director/Sig-III	RDSO	Member	Recommend
Rajendra Dhambel PED/S&T	RDSO	Approving Authority	Approved

AMENDMENTS:

Specification No.	Version	Amendment	Amendment Details	Effective date
RDSO/SPN/211/2022	1.0		First Issue	24.11.2022

Table of Content

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 Multiplexer 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**

2.2.1	FNmux	Fail-Safe Network Multiplexer
2.2.2	UFSBI	Universal Fail-Safe Block Interface
2.2.3	FNmux(CU)	FNmux (Central Unit)
2.2.4	FNmux(FU)	FNmux (Field Unit)
2.2.5	CU	Central Unit
2.2.6	FU	Field Unit
2.2.7	MTBF	Mean time between Failure
2.2.8	MTTF	Mean Time to Failure
2.2.9	MTBWSF	Mean Time between Wrong Side Failures
2.2.10	CENELEC	European Committee for Electro technical Standardization
2.2.11	EN	European Standards
2.2.12	IEEE-SA	Institute of Electrical and Electronics Engineers Standards Association

2.2.13	IEEE 802.3	IEEE 802.3 specifies the physical and networking characteristics of an Ethernet network, like how physical connections between nodes (routers/switches/hubs) are made through various wired media like copper coaxial or fiber cable.
2.2.14	SIL-4	Safety integrity level - 4
2.2.15	EMF	Electro-Motive force

3 APPLICABLE DOCUMENTS

Sl. No.	Subject	Specification
1	EN50126	Railway Application Specifications and Demonstration of Reliability, Availability, Maintainability & Safety
2	EN 50128	Railway Applications-Communications, Signaling and processing systems-Software for Railway Control and Protection Systems.
3	EN 50129	Railway Applications-Communications, Signaling and processing systems- Safety Related Electronics Systems for Signaling.
4	EN50159	Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
5	EN 50121-4	Electromagnetic compatibility - Emission and immunity of the signalling and telecommunications apparatus
6	EN 50124-1	Railway applications – Insulation coordination
7	EN 50125-1	Railway applications - Environmental conditions for equipment
8	EN 50125-3	Railway applications - Environmental conditions for equipment Part 3: Equipment for signalling and telecommunications
9	EN 50155	Railway Application – Electronic equipment used on Rolling stock.
10	IEC 62236-2	Compatibility – Part 2: emission of the whole railway system to the outside world
11	RDSO/SPN/144	Safety and reliability requirement of electronic signaling equipment.
12	IRS: S 36	Relay Interlocking systems
13	IRS: S 23	Electrical Signaling and Interlocking Equipment
14	RDSO/SPN/192	Electronic Interlocking
15	IRS:S-104/2012	Universal Fail-Safe Block Interface

16	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 signaling circuits using electronic equipment as laid down in Signal Engineering Manual IRSEM Issue July 2021 and as stipulated in RDSO/ SPN/144/2006 or latest.

4.2 The system shall comply with the specification no. RDSO/SPN/144/2006 or 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^{o}C to +70^{o}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 or 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, RDSO/SPN/215/2018 Ver.2.0 or latest & relevant IEC standards.

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.

4.12 It shall be IP65 compliant.

4.13 The size of the FU equipment shall be such that it will be able to accommodate in full location boxes in the field.

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 -CU) to concentrate I/O from the distributed field modules (FNmux Field Unit -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. Vital cards can be used for non-vital I/O information also. The system should also be able to communicate with Data Logger.

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** architecture in standalone mode or **2oo3** architecture as per EN 50129. However, the system shall be provided with hot standby configuration for enhanced reliability. Other module of the central unit shall have CENELEC SIL-4 compliant fail-safe architecture with minimum 8/16 digital I/O scalable to 256 I/O or as per purchaser's requirement for transferring of vital signal, tracks and other similar vital relay status. The Central Unit should be modular in nature and expandable up to minimum 256 digital I/Os or as per purchaser's requirement. The system must maintain safety level of SIL-4 even during the failure/ removal of all redundancies. It should be capable of transmitting and receiving information from CU to CU and CU to FUs (multipoint).

   The removal and plugging of redundant processor module must be hot swappable and should not require shutting down of system. It shall be possible to place redundant processor module at two different and independent places without affecting the performance, safety and reliability of the system.

   There shall be possibility of placing the central unit in field location boxes in case of emergency.

   The transfer to hot standby system should be seamless, without affecting safety & ongoing operations.

b) **FNmux Field Unit (FU):** Each module shall have CENELEC SIL-4 compliant fail-safe architecture, configuration with at least 8/16 (or as per purchaser's requirement) 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 signal, tracks and other similar vital relay status. FNmux Field Unit shall be able to transfer vital information to CU. This should be DIN Rail or with any other suitable mountable device along with Power supply and communication switch.

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 with maximum response time of less than 1 second.

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

5.1 FNmux Central Unit (CU):

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

5.1.1 The equipment shall be compatible with 12V/24V/60V DC (+20% to -30%) signal driven systems like relays, indication lamps etc.

5.1.2 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.

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

5.1.4 The FNmux Central unit shall cater minimum 8/16 inputs and 8/16 outputs (or as per purchaser's requirement) & shall be scalable up to minimum 256 Inputs and 256 outputs (or as per purchaser's requirement) by addition of modules. Each output port shall be capable to drive signaling relays using internal power supply, for the purpose of sensing inputs, potential free contacts of relays shall be used.

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

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

5.1.7 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 1 seconds.

5.1.8 The pair of equipment shall be transparent to the signaling circuit / equipment connected through them.

5.1.9 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 or MAC IP or IP Address or DIP switches.

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

5.1.11 FNmux Central Unit (CU) shall be self-diagnostic system and shall be capable of interfacing with maintenance terminal or any PC to fetch the

required information.

5.1.12 It should be capable of transmitting and receiving information from CU to CU and CU to FUs (multipoint).

5.1.13 LED indications shall be provided on modules for all inputs and outputs to indicate its status and errors.

5.1.14 The CU shall preferably be located in the station building, Relay hut or Gate lodge**.** However the dimension of CU should be such that in case of non-availability of building/room/space or in case of emergency, it can be located in field location boxes also. Therefore the Central Unit FNmux must comply with EN 50121- 4 (Electromagnetic compatibility), EN 50124-1 (Insulation coordination), EN 50125-1 (Environmental condition), EN 50125-3 (Environmental condition), EN 50155 (Vibration).

5.2 FNmux Field Unit (FU):

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

5.2.2 The equipment shall be compatible with 12V/24V/60V DC (+20% to -30%) signal driven systems like relays, indication lamps etc.

5.2.3 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 safe Ethernet protocol must be as per CENELEC standard EN 50159 to make the complete system SIL-4 certified as per CENELEC EN 50129. 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.

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

5.2.5 Field Unit (FU) shall have CENELEC SIL-4 compliant fail-safe architecture. Each Vital Trackside Module shall have at least 8/16 inputs scalable to 64 inputs and 8/16 outputs scalable to 64 outputs (or as per purchaser's requirement) using single or scalable modules. Each output port shall be capable to drive all type of signaling Q Series/12/24/60V DC Signaling relays and using internal power supply for the purpose of sensing inputs, potential free contacts of relays shall be used. This should be DIN Rail or with any other suitable mountable device along with power supply and communication switch.

5.2.6 Each output/Input shall have suitable protection for back E.M.F./Short

ckt /Overload etc.

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

5.2.8 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.

5.2.9 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 or MAC IP or IP Address or DIP switches.

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

5.2.11 The Field Unit FNmux must comply with EN50121- 4 (Electromagnetic compatibility), EN 50124-1 (Insulation coordination), EN 50125-1 (Environmental condition), EN 50125-3 (Environmental condition), EN 50155 (Vibration)

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 and back contacts both). 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 (both + and -) using Internal power supply with suitable protection .The Relay output module shall drive isolated output.

5.3.4 The read back facility should be provided to monitor the status of the relay vis-à-vis the CU's information.

5.4 NETWORK ARCHITECTURE

5.4.1 The system comprised of the vital modules shall be capable to work on dual redundant OFC Ring Network using Managed Layer 2

Ethernet switch with applicable protocol suite, with 10/100/1000 Mbps Ethernet or any other suitable and proven protocol for safety systems.

The Ethernet switch shall work on the same power supply as that of the CU/FU itself.

Schematic block diagram is given in figure-1 .

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

(i) 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.

(ii) Wide Temperature operation: -10 ^{0}C to +70 ^{0}C.

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

5.4.2 The network elements of industrial grade 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 or 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.

5.4.4 Internal data logger facility shall be provided for failure analysis. Information of all the Inputs and Outputs sensed or driven by an FNmux network (either through the Central Unit or remote Field Units) must be available at the FNmux Central Unit, in an Open or Standard protocol for easy connectivity to Network Datalogger (for diagnostic purposes) either directly or through suitable protocol converters.

5.4.5 The remote monitoring software shall be browser based and shall be transparent across the makes. Remote Diagnostics terminal with NMS facility should be available for each FNmux network installed, where all the health parameters, error messages and I/O's of each remote Field Unit and the Central Unit can be monitored.

5.4.6 Seamless change over from one path to another path or from one medium to another medium shall be possible.

5.5 POWER SUPPLY MODULE

5.5.1 The power supply module shall work with input voltage of 24 V DC / 110 V DC / 110 VAC as specified by the purchaser 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. SPD provided shall be as per specification no. RDSO/SPN/215/2018 Ver.2.0 & relevant IEC standards.

vii) The complete FNmux system, vital field modules and Central cluster 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.) as per 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 in safe standby mode with all output getting de-energized. This will resume automatically once the proper packets are received after resuming the link.

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 12V/24V/60V DC 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 Vital 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 cluster vital modules) 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 within 1 second 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 a 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. Any single fault should bring system to safe state.

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 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 up to serial data rate equivalent to 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. SPD provided shall be as per specification no. RDSO/SPN/215/2018 Ver.2.0 & relevant IEC standards.

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

(x) FNmux shall be capable of interfacing with EI, Axle counter, TPWS, ETCS, TCAS (as SIL-4 RIU), Radio Block Centre & CTC/TMS (as FIU) and other advance systems using standard protocols.

(xi) The FNmux must communicate with other signaling devices on RASTA protocol. Therefore, FNmux must be RASTA protocol ready. Till such time all other signaling devices are ready with RASTA protocol, FNmux must communicate using suitable standard international protocols available.

8 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. The Software tool used for developing software should be SIL-4 certified or ISA approved as per CENELEC standard. 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 all the functionalities defined in the scope. 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 processor is 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.
d) Any other techniques approved by ISA as per CENELEC EN 50126, EN 50128, EN 50129 and EN 50159 all combined together.

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 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 Or Suitable Programmer with computer interface.
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 as per ISA guidelines and type test format.
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 as per ISA guidelines and acceptance test format.
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/144/2006 or 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 or Latest.

10.9 Applied High Voltage Test

Applied High Voltage Test shall be carried out as per relevant clause of RDSO/SPN/144/2006 or 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 or Suitable Programmer with computer interface.
viii) UV Eraser if required.

ix) Microprocessor development system or IDE 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 or Latest.

14 INFORMATION TO BE SUPPLIED BY THE MANUFACTURER

14.1 Documentation as per relevant clause of RDSO/SPN/144/2006 or 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

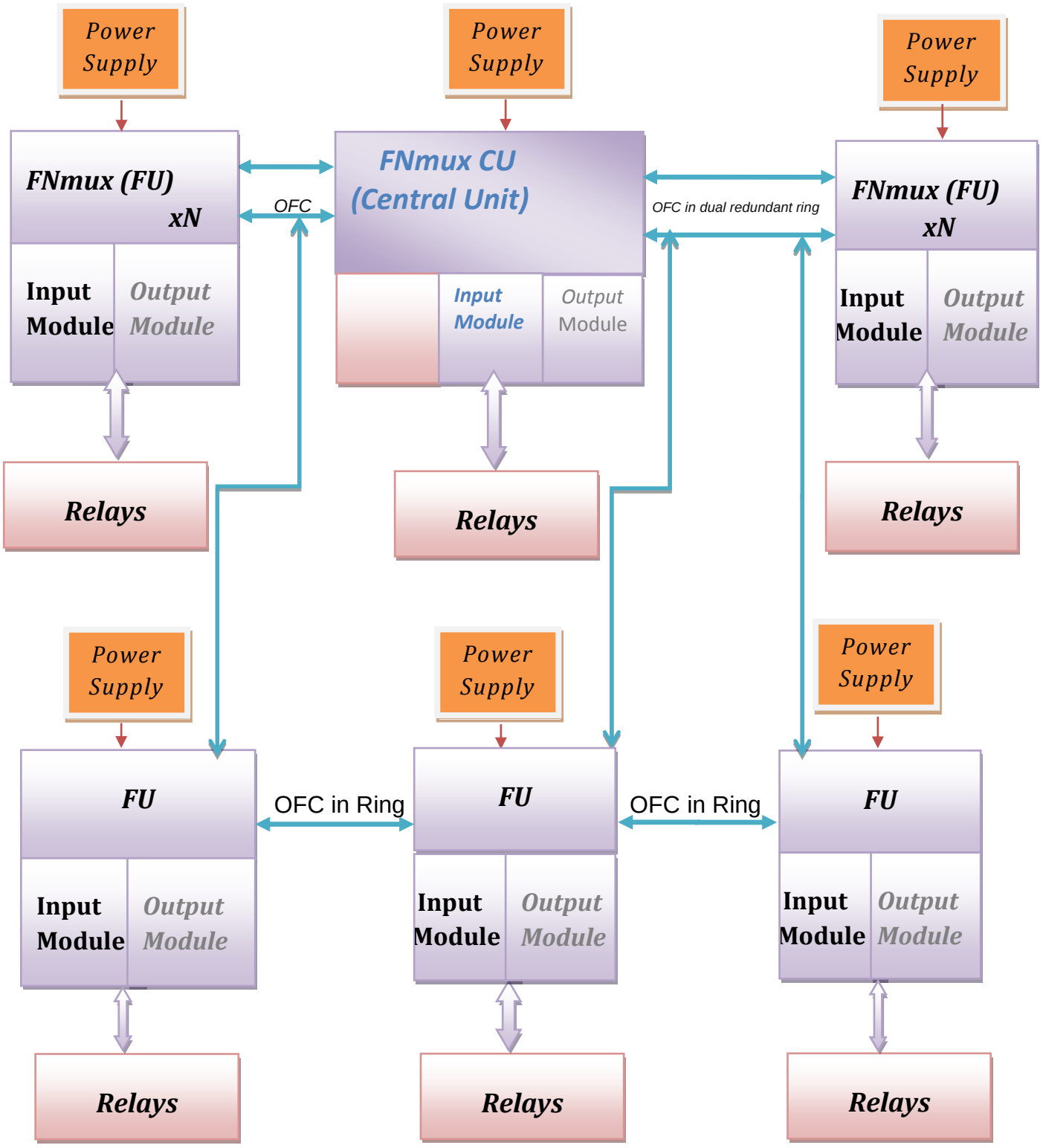
a) Medium on which FNMUX is intended to work single/dual OFC
b) Depending on the inter nodal distance, the type of OFC cable (Single / Multi mode) used.
c) Whether there shall be Dual Redundant OFC ring through diverse routes or only a single ring.
d) Numbers of inputs & outputs and application.
e) The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

16 VENDOR-CHANGES IN APPROVED STATUS:

(Compliance of Document No - QO-D-8.1-11)

All the provisions contained in RDSO's ISO procedures laid down in Document No. QO-D-8.1-11 (title "Vendor-Changes in approved status") and subsequent versions/amendments thereof, shall be binding and applicable on the successful vendors in the contracts floated by Railways to maintain quality of products supplied to Railways.'

****



Block Working Diagram of CU with FU