

2724589/2024/O/o PED/TI/RDSO



सत्यमेव जयते

भारत सरकार GOVERNMENT OF INDIA

रेल मंत्रालय MINISTRY OF RAILWAYS

अनुदेश संख्या: टीआई/आईएन/0048

Instruction No: TI/IN/0048

भारतीय रेल में पुरानी विशिष्टियों के अनुसार प्रयुक्त

वर्तमान स्काडा प्रणाली में

साइबर सुरक्षा के कार्यान्वयन के लिए

तकनीकी अनुदेश

Technical Instruction for implementing

Cyber Security in existing

Supervisory Control and Data Acquisition System

used in Indian Railways as per old Specifications

अप्रैल, 2024 में जारी / Issued in: April, 2024

		हस्ताक्षर/Signature
अनुमोदित Approved by	प्रधान कार्यकारी निदेशक (कर्षण संस्थापन) Principal Executive Director (TI)	<i>Am 7/1/24</i>

जारी कर्ता/ISSUED BY:

कर्षण संस्थापन निदेशालय

TRACTION INSTALLATION DIRECTORATE,

अनुसंधान अभिकल्प और मानक संगठन

RESEARCH DESIGNS & STANDARDS ORGANISATION,

मानक नगर, लखनऊ- 226011

MANAK NAGAR, LUCKNOW-226011

NOTE: This guideline is the property of RDSO. No reproduction shall be done without the permission of DG (TI) RDSO.

	Prepared By	Checked By	Issued by
Signature	<i>Vikaash</i>	RAMESH	<i>Kumar</i>
Date	18.04.2024	KUMAR PAL	18/4/24
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO

1 Scope & Objective:


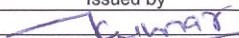
This technical instruction is applicable to different types of existing SCADA Systems provided on Indian Railways. The objective of this technical instruction is to upgrade the existing SCADA System in line with Cyber Security and to identify the migration path for the prevalent systems to a system where Cyber security requirements as per the latest specification TI/SPC/RCC/SCADA/0134 are to be achieved to the maximum extent possible with least amount of replacement/retrofitting.

2 Introduction

Presently the Traction SCADA systems prevalent in Indian Railways are as per the following RDSO specifications –

- i. TI/SPC/RCC/SCADA/0990: This is based on the SPORT Protocol and was issued on August 08, 2008.
- ii. TI/SPC/RCC/SCADA/0130 (or 0130 Rev1): This is based on the IEC-101 Protocol, supporting the IEC-103 Protocol to integrate protection relays. It was issued on December 12, 2014.
- iii. TI/SPC/RCC/SCADA/0130 Rev2: This is based on IEC-104 Protocol using E1 communication channels. It was issued on July 26, 2016.
- iv. TI/SPC/RCC/SCADA/0133: This specification adds support for the IEC 61850 protocol for integration with protection relays and basic cyber security requirements. It was issued on July 30, 2021.
- v. TI/SPC/RCC/SCADA/0134: This specification incorporates the Cyber Security features to address the Cyber Security vulnerabilities present in the SCADA System. It has been issued on November 09, 2023.

The SCADA System of Indian Railways has been declared as Critical Information Infrastructure (CII) as per directives of National Security Council Secretariat (NSCS), Government of India and Railway Board vide letter No. 2003/Elect (G)/161/1 Vol-III/Pt- Part (4) dated 13.04.2022, had advised RDSO to incorporate the Cyber Security Features in SCADA Specification to address the Cyber Security Vulnerabilities present in the SCADA System. Accordingly, the revised SCADA Specification TI/SPC/RCC/SCADA/0134 incorporating various Cyber Security features has been issued on 09.11.2023 and in view of the same, this technical instruction has been prepared to implement Cyber Security features in the existing SCADA systems as per the specification mentioned above at SN- i. to iv. present in the Indian Railways to the maximum possible extent.

	Prepared By	Checked By	Issued by
Signature		RAMESH KUMAR PAL	
Date	18.04.2024	20.03.2024	
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO

3 Implementation of Cyber Security in 0990 Systems:

3.1 Methodology

Since these are the oldest working versions of the SCADA System, it is not possible to completely implement Cybersecurity requirements. As this specification has been superseded by Specification TI/SPC/RCC/SCADA/0130 Rev.1 dated December 12, 2014, therefore, most of the SCADA systems working in Indian Railways as per this specification are near the end of their codal life. **The SCADA system, which has completed 75% of its codal life (from the date of Commissioning), for such systems, the entire RCC and RTU may be replaced as per the governing specification TI/SPC/RCC/SCADA/0134 or the latest.**

However, for systems where 75% of Codal Life is not yet completed, an intermediate approach as proposed below shall be adopted -


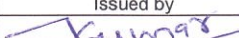
- i. Since these systems are based on Windows 7, therefore, RCC (complete hardware and software) shall be replaced, i.e., a system identical to the one specified in the Specification TI/SPC/RCC/SCADA/0134 or latest shall be adopted. For RCCs, where multiple such systems exist, the feasibility of merging those into a single system (up to 100 RTUs) shall also be considered.
- ii. Communication links to be upgraded from FSK modem-based channels to E1-based Ethernet channels (This will be provided by the S&T wing of Railway). This will bring all RTUs at par, as currently TSS RTUs are on E1 channels and SP/SSP RTUs are on FSK modem channels.
- iii. For RTUs that have completed 75% of Codal Life, these RTUs may be replaced as per the latest specifications.
- iv. For RTUs that have not completed 75% of their codal life, the following may be implemented-
 - a. Protocol converters shall be installed at each RTU that convert the SPORT protocol of the RTU into secure (encrypted) IEC-104 for compatibility with the new RCC.
 - b. When the Codal life of this RTU is completed, it may be replaced with the latest specification RTU with minimal configuration changes at RCC software.

NOTE: In most of the locations, TSS RTUs have already been replaced as per TI/SPC/RCC/SCADA/0130 Rev2, and hence it would not require further replacement. Only the firmware of the RTU needs to be upgraded to achieve the security requirements in line with the Specification TI/SPC/RCC/SCADA/0134 or the latest.

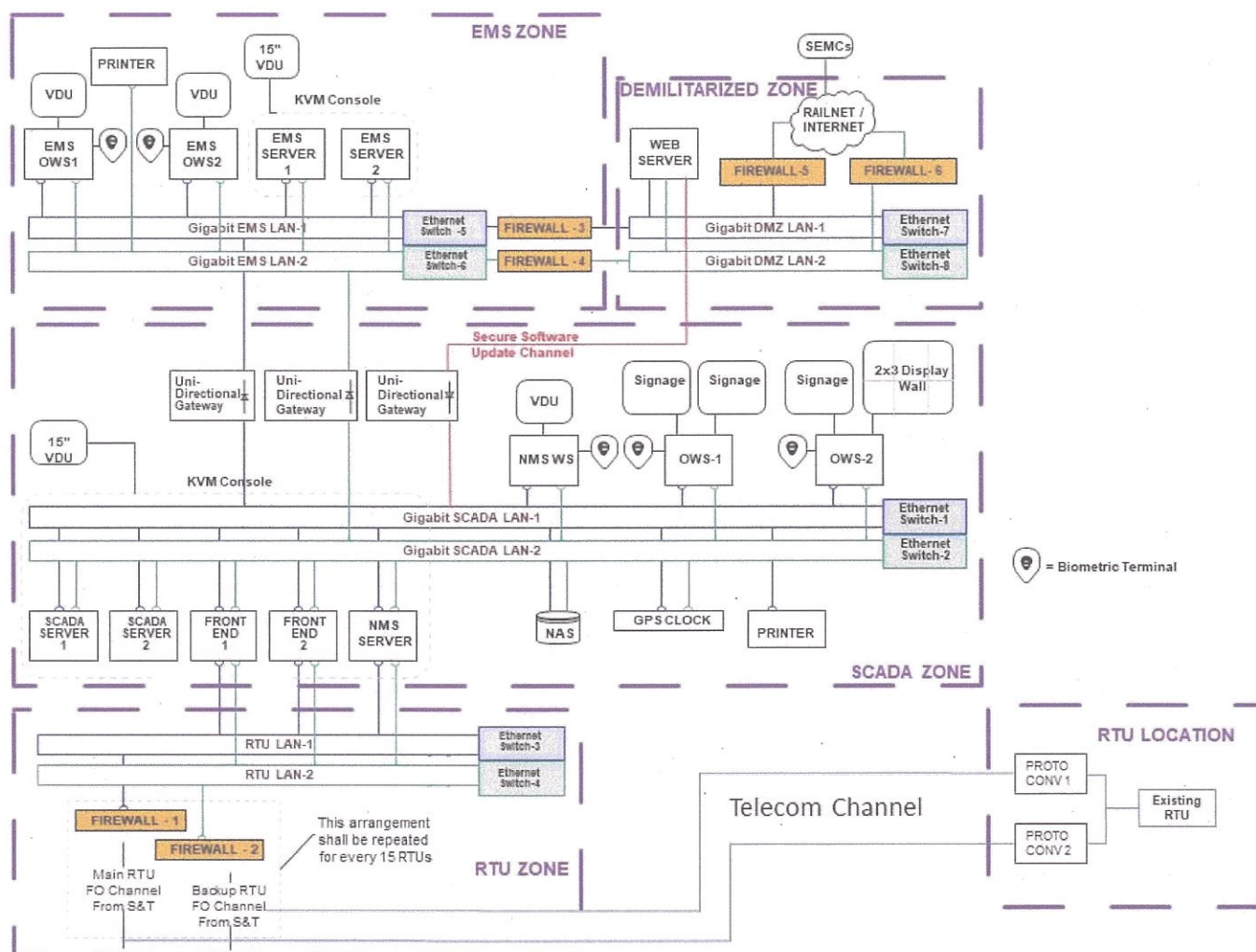
3.2 Protocol Converter Specifications

The Secure (encrypted) IEC-104 protocol converter for existing RTUs shall have the following minimum functions-

- Communicate as SPORT master with existing RTU to perform status, telemetry acquisition, and control functions.
- Convert SPORT protocol data into IEC-104 format and send it to RCC.
- Support Secure IEC-104 protocol as per IEC 62351-3 and IEC 62351-5 towards RCC.
- Receive control commands from RCC on Secure IEC-104 and transfer to RTU on SPORT.
- Two units to be provided to operate in hot-standby mode so that failure of one converter does not lead to loss of RTU functions.

	Prepared By	Checked By	Issued by
Signature		RAMESH	
Date	18.04.2024	KUMAR PAL	
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO



GENERAL ARRANGEMENT OF MASTER STATION COMPUTER FOR 0990 SYSTEM

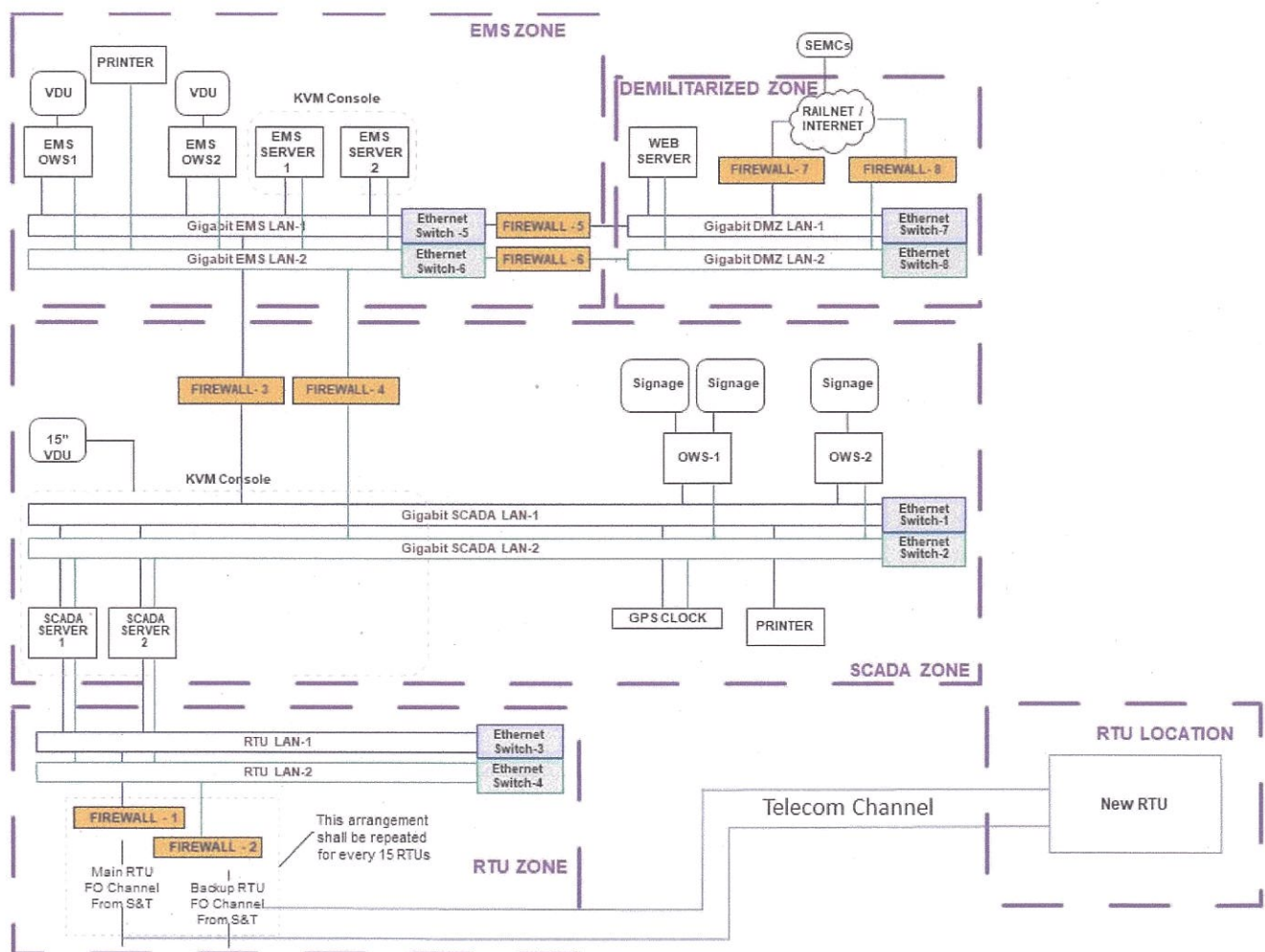
	Prepared By	Checked By	Issued by
Signature	Vikash	RAMESH	Kumar
Date	18.04.2024	KUMAR PAL	
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO

4 Implementation of Cyber Security in 0130 Rev1 Systems.

Since the population of SCADA Systems based on this specification is very small in Indian Railways, therefore, for systems on this specification, an approach as proposed below may be adopted-

- Communication links to be upgraded from FSK modem-based channels to E1-based Ethernet channels. This will bring all RTUs at par, as currently TSS RTUs are on E1 channels and SP/SSP RTUs are on FSK modem channels.
- Upgradation of RCC hardware is not required, and existing hardware shall be reused.
- RCC software shall be upgraded as per specification TI/SPC/RCC/SCADA/0134 or the latest.
- Ethernet Switches and firewalls as per specification TI/SPC/RCC/SCADA/0134 or latest shall be installed at respective interconnections.
- RTU shall be replaced as per specification TI/SPC/RCC/SCADA/0134 or latest.



**GENERAL ARRANGEMENT OF MASTER STATION COMPUTER FOR 0130 (Rev.1)
SYSTEM**

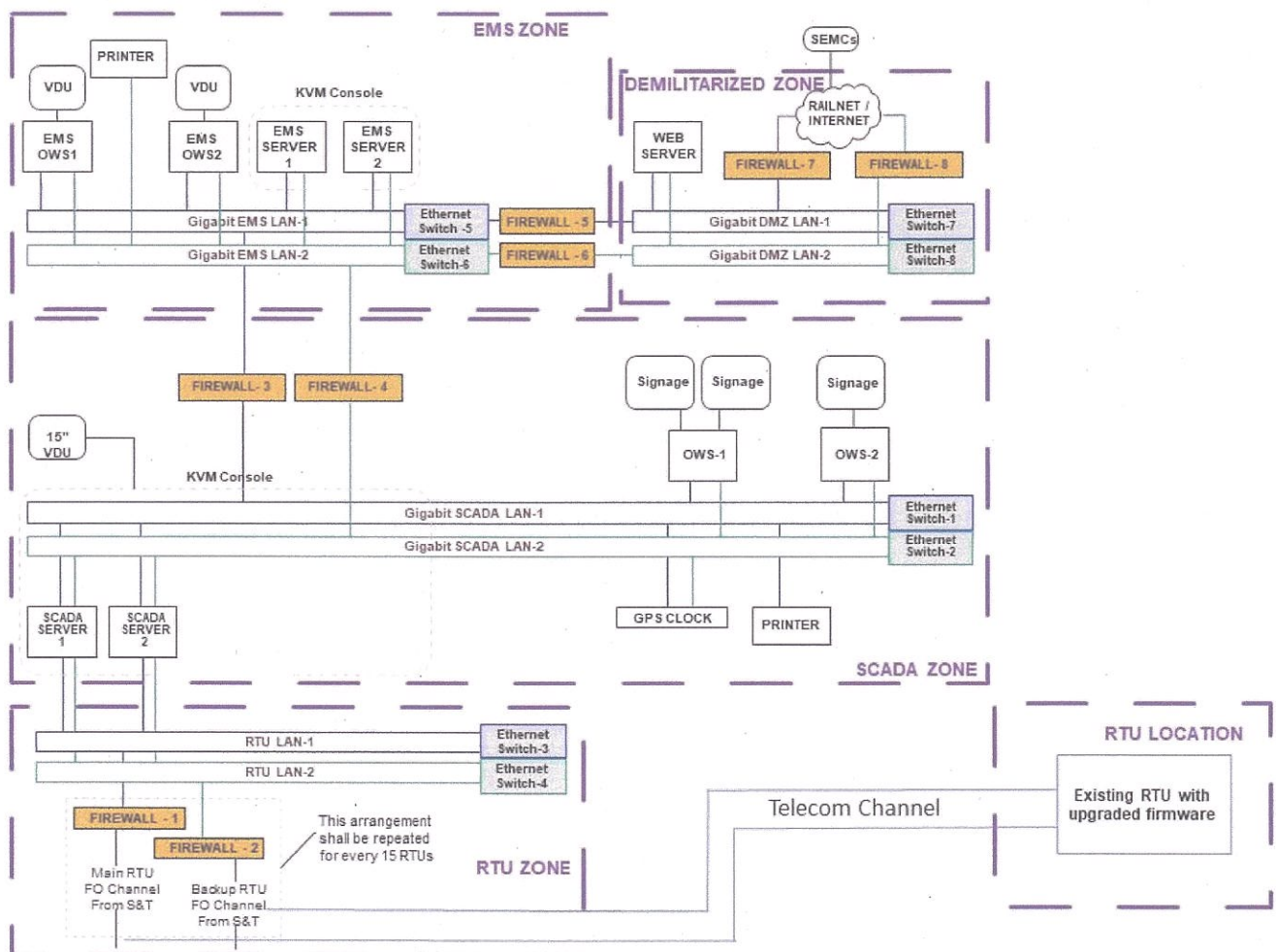
	Prepared By	Checked By	Issued by
Signature	Vikash	RAMESH	Kumar Pal
Date	18.04.2024	KUMAR PAL	
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO

5 Implementation of Cyber Security in 0130 Rev2 Systems

The SCADA system belonging to this specification has major population in Indian Railways. Therefore, for such systems, the approach proposed below shall be adopted:

- Upgradation of RCC hardware is not required, and existing hardware shall be reused.
- RCC software shall be upgraded as per specification TI/SPC/RCC/SCADA/0134 or latest e.g., alphanumeric password protection, Identification and authentication control, patch management, application whitelisting, etc shall be incorporated.
- Ethernet Switches and firewalls as per specification TI/SPC/RCC/SCADA/0134 or latest shall be deployed at respective interconnections at RCC.
- For RTUs, firmware shall be upgraded to support encryption in IEC-104 protocol to secure the communications between SCADA and RTUs.



GENERAL ARRANGEMENT OF MASTER STATION COMPUTER FOR 0130 (Rev.2) SYSTEM

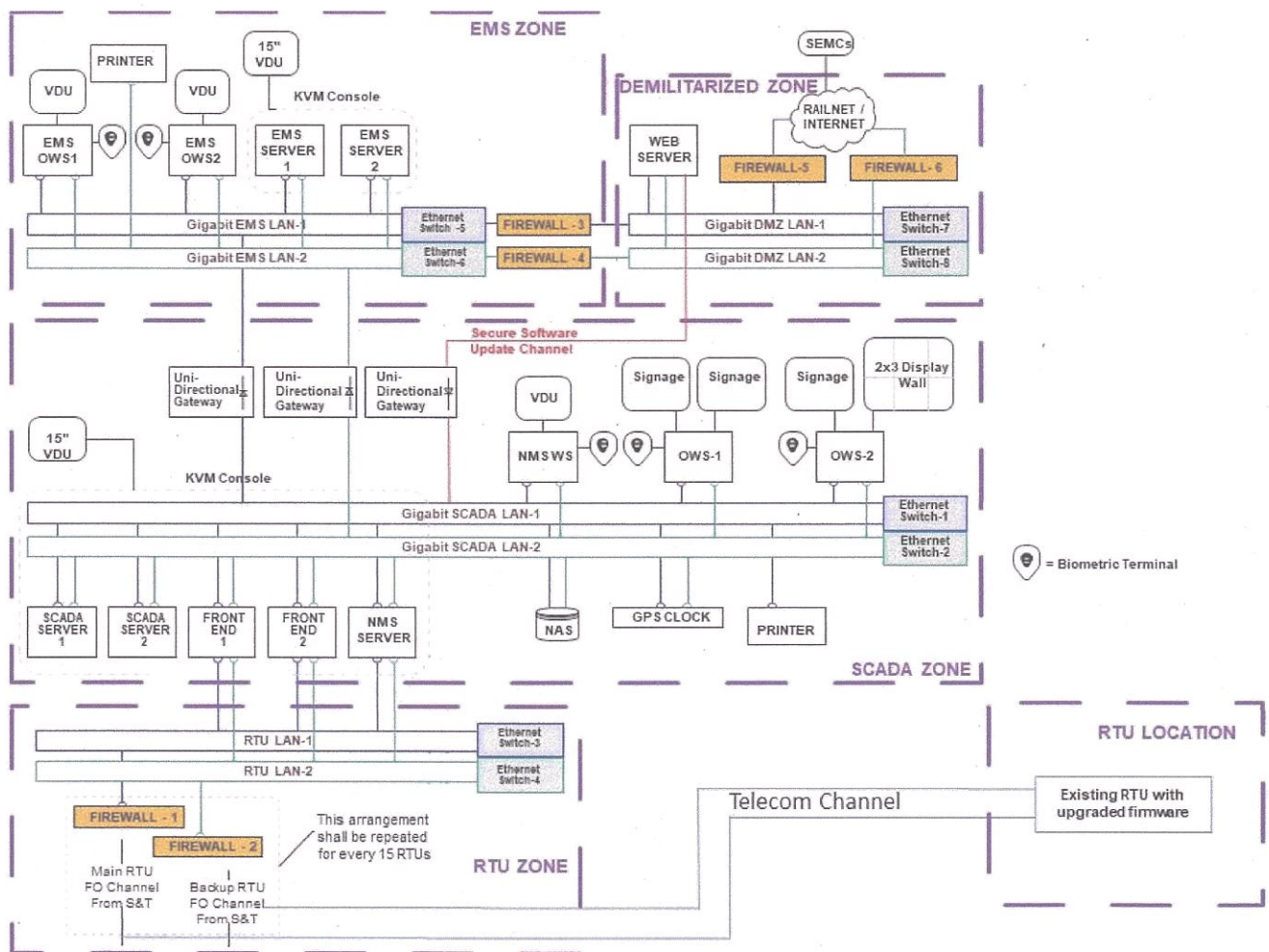
Signature	Prepared By	Checked By	Issued by
Date	18.04.2024	RAMESH KUMAR PAL	
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO

6 Implementation of Cyber Security in 0133 Systems:

This specification was issued in July 2021. As this is a recently issued specification, there are very few systems of this type for which the approach as proposed below shall be adopted –

- Upgradation of RCC hardware is not required, and existing hardware shall be reused.
- RCC software shall be upgraded as per specification TI/SPC/RCC/SCADA/0134 or the latest.
- Ethernet Switches and firewalls as per specification TI/SPC/RCC/SCADA/0134 or latest shall be deployed at respective interconnections.
- Biometric terminals shall be added as per specification TI/SPC/RCC/SCADA/0134 or latest.
- For RTUs, firmware shall be upgraded to support encryption in IEC-104 protocol to secure the communications between SCADA and RTUs.



GENERAL ARRANGEMENT OF MASTER STATION COMPUTER FOR 0133 SYSTEM

Signature	Prepared By	Checked By	Issued by
Date	28.04.2024	RAMESH KUMAR PAL	<i>[Signature]</i>
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3

2724589/2024/O/o PED/TI/RDSO

7. Time Synchronization:

SCADA System, for synchronization of their ICT clocks, shall be time synchronized with Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory(NPL) or with NTP servers traceable to these NTP servers. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however, it is to be ensured that their time source shall not deviate from NPL or NIC. CERT-In guideline issued vide No. 20(3)/2022-CERT-In dated 28.04.2022 shall be followed in this regard.

8. Cyber Security Audit of the Upgraded SCADA System:

SCADA vendors shall ensure to conduct Cyber Security Audit after upgradation of the existing SCADA System in terms of Cyber Security requirements, and thereafter annually, by the government agency/government approved third party agency/CERT-In empanelled Information Security Auditing Organization. Any vulnerabilities identified during the audit shall be rectified by the SCADA vendor and get revalidated by the corresponding auditing agency.

Zonal Railways shall specifically include the Cyber Security audit in their tender documents while planning the works related to the implementation of Cyber Security in existing SCADA System.

	Prepared By	Checked By	Issued by
Signature	Vikash	RAMESH Digitally signed by RAMESH KUMAR PATEL DN: cn=RAMESH KUMAR PATEL, o=RAILWAYS, ou=RAILWAYS, c=IN	Kuldeep
Date	18.04.2024		
Designation	JE/ TI	ADE/ TI-3	DIRECTOR/ TI-3