Technical Advisory Note (TAN)			
Subject	**Comprehensive Security Guidelines for CCTV Network.**		
Doc. No.	STT/TAN/CCTV/2024	Version – 1.0	Date – 24.04.2024

1. Scope:

1.1. This document provides guidelines for Regular Security Audit by the Zonal Railways of the complete CCTV network of Railways.

1.2. This document also specifies procedure to ensure that the IP based CCTV cameras of same make and model (Camera SoC & Camera Firmware) are being supplied for Type Test/ Acceptance Test by the OEM/ Vendor/ Firm which were certified by STQC.

2. General Requirements:

A Video Surveillance System (VSS), also known as Closed-Circuit Television (CCTV) System, is a collection of cameras and other related equipment used to monitor and record activities in a specific area commonly used for security and surveillance purposes.

2.1. General best practices to be followed to secure the CCTV network. Regular cybersecurity audit of network by **Zonal Railways** is to be done to identify vulnerabilities, optimize system performance and ensure that the system is operating effectively and securely.

2.2. The CCTV cameras (IoT device) are being audited for cybersecurity aspect by STQC at the time of initial procurement, installation & commissioning and certification is being issued.

2.3. Based on the above-mentioned certification and requirement of Railways these CCTV cameras are inspected and checked for compliance of various parameter mentioned in the RDSO specification by concerned QA/S&T RDSO field units.

2.4. Complete CCTV network of Indian Railways (IR) over Railway Stations should be on the INTRANET network of Railway and should not accessible through internet directly. RDSO Specification has provided the safeguard for viewing the camera feed on mobile by VPN as done in other railway applications like e-office etc.

2.5. No provision of wireless connectivity should be available in the camera. The data should be shared across Indian Railway network through Servers connected to the INTRANET network of Railway.

2.6. The Rules and regulations as applicable, notified by the Government or procurement of goods and services must be followed, e.g.

a) Public procurement Order (Make in India), 2017 or latest.
b) Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021 or latest.

2.7. The purchaser should ensure that latest orders issued by Government of India related to CCTV network are followed. In case any breach or false declaration is found at any stage, immediate strict penal action is to be initiated by the purchaser.

3. Important aspects for auditing of CCTV Network:

3.1 Asset Monitoring and Network Audit:

3.1.1 CCTV Network should be audited atleast annually from a CERT-In empanalled Information security Auditing Organsiation like STQC for minimizing security threat. This will also ensure hardening of CCTV network on annual basis..

3.1.2 The CCTV System should have auto discovery tool to collect information about all IP devices (Cameras, Switches, Servers, NVR, Storage, Workstations UPS etc) connected on the network. Auto discovery also ensures to generate alert when new devices are introduced on your network for monitoring them for any suspicious activity. It should also generate alert whenever a device is detached from the network.

3.1.3 Authorized Users should have end-to-end visibility of CCTV network through Enterprise grade Network Management System.

3.1.4 To avoid false alarms, alarm notification function in CCTV surveillance cameras to be checked and verified as per the laid-out plans and security protocols.

3.2 Physical Security:

3.2.1 CCTV network infrastructure should be accessed by authorized users only. Physical access is an important security control to prevent from adding malicious devices onto the network to enable reverse shells or remote access.

3.2.2 Implement access control measures for areas containing critical network infrastructure, like biometric access to server rooms can be done or Register of entry and exit to the control rooms, etc. should be maintained.

3.2.3 Network cables should not be exposed or within easy reachand shall not pose a risk of being easily cut. Also, switch racks should be kept locked, positioned at proper heightand should not allow easy access to cables and ports. Network cables and network-switch racks should be secured so as to prevent unauthorized access or tampering.

3.3 Blocking of Open Ports:

3.3.1 One of the most common techniques used by attackers is to scan for open ports to identify possible ways to gain network access. CCTV network should be regularly checked for open ports to discover what network services are enabled.

3.3.2 Unused ports on the network switches should be blocked.

3.4 **Security Hardening:**

3.4.1 Firewalls should be used and configured only to allow necessary traffic.

3.4.2 Periodically review firewall configuration, rules, and policies. Ensure that only authorized employees can access the firewall.
Protect administrative access with following measures to ensure that access is controlled with the highest security requirements:

i. Identify privileged accounts.
ii. Assign privileges based on roles.
iii. Implement the principle of least privilege.
iv. Use multi-factor authentication.
v. Use strong passwords.

3.4.3 Default passwords should be avoided and changed immediately.

3.4.4 Strong password policies should be enforced for all devices and user accounts, including regular password changes and the use of complex passwords.

3.4.5 If any traffic from CCTV Network to internet is required then it should be routed through firewall by using NAT only.

3.4.6 Implement MAC-Port binding to restrict access to only known devices to specific ports on switches.

3.5 **Manage and Restrict Admin Access:**

3.5.1 Attackers are always looking for Admin Access, especially credentials allowing full network access that enable an attack path to elevate privileges.

3.5.2 Remove and revoke excessive Admin privileges regularly

3.6 **Remove Unused Devices:**

3.6.1 Unused devices on the network typically get forgotten and are often left with vulnerabilities such as weak credentials, becoming prime targets for attackers to gain access and elevate privileges. As part of audit and inventory discovery process, all unused devices that are no longer required, should be removed.

3.7 **Regular Monitoring and Log Analysis:**

3.7.1 Monitor the CCTV system logs for unusual activities and potential security breaches.

3.7.2 All network access requests should be monitored closely to check unusual or suspicious activity.

3.7.3 All activities should be logged for a period of minimum 180 days period.

3.8 **Software Update:**

3.8.1 Software Updates for the devices within CCTV network should be done based on the severity and risk of vulnerabilities following the industry best practices.

3.8.2 Camera firmware and all other STQC verified software should be updated only after receiving security certification from STQC for new firmware/software version. The CCTV system should be configured for centralized updation of firmware of cameras & CCTV infra.

3.9 **Disable Unused Software and Services:**

3.9.1 Unused services and software can be a high risk to the CCTV Network, especially when left unpatched or not updated to later versions.

3.9.2 This can leave weak configurations, default credentials, or vulnerabilities that can open doors for attackers to gain unauthorized access to sensitive systems and data.

3.9.3 Periodically review service lifecycle and software catalog to determine which services and software can be removed.

3.9.4 Remote access applications like AnyDesk, Team-Viewer, etc. shall be removed from the hosts.

3.9.4.1 In case, remote access is required for maintenance or monitoring, remote connections should be provided through a secure VPN (Virtual Private Network). Exposing the system directly to the internet should be avoided.

3.10 **Network segmentation:**

3.10.1 A separate VLAN instances should be created on switches for different type of services (CCTV, display network, Wi-Fi etc) and access switches should separate these services in form of unique VLANs & maintain a logical segregation between these services.

3.10.2 This will maintain each service separately from traffic flow and QoS implementation perspective and improve network performance along with securing and isolating these services from each other.

3.10.3 Details of Typical VLAN for CCTV Network for Indian Railways is enclosed as Annexure-A

3.11 **Encryption of Data**

3.11.1 It should be ensured that all communication between cameras, recorders, and viewing devices is encrypted. This shall prevent unauthorized individuals from intercepting and accessing sensitive information.

3.11.2 For optimal security protocols, Cameras should be configured utilizing HTTPS, a secure communication protocol that encrypts data transmission between the camera and client, thereby safeguarding confidentiality and integrity. Additionally, implementation of streaming protocols (RTSP/ FTPS/ HLS) over HTTPS ensures the secure transmission of video data.

3.12 **Data Storage & Retention:**

3.12.1 It shall be ensured that proper data storage and retention policies are in place. Securely store recordings and define how long data should be retained before it gets automatically deleted. Data Storage should be in terms of storage duration (number of Days - minimum 30 days as specified in RDSO specification) based on operational requirements rather than storage capacity. The data storage of all CCTVs installed at Government Establishment/ Public Places should be mandated to be within the India even if it is stored in cloud platforms.

3.13 **Staff Training:**

3.13.1 Provision of comprehensive training to employees and system administrators on security best practices should be emphasized through OEM to make them understand the potential risks and how to mitigate them effectively.

3.14 **Verification of SoC & Hash value of firmware of the cameras:**

3.14.1 The Security Audit certification/ report contains HASH value of the tested firmware & SoC Name/ Number of the tested hardware by the lab and it is mentioned on certification/ report.

3.14.2 These shall be verified by RDSO during TT & AT.

3.14.3 The procedure for verification of HASH value & SoC of the camera is enclosed as Annexure-B.

Technical Advisory Note (TAN)			
Subject	**Comprehensive Security Guidelines for CCTV Network.**		
Doc. No.	STT/TAN/CCTV/2024	Version – 1.0	Date – 24.04.2024

Annexure-A

1. VLAN for CCTV Network for Indian Railways:

1.1. A virtual local area network (VLAN) is a logical network formed within a physical network infrastructure. VLANs for CCTV Network of IR, create a logical -- or virtual -- subnet of devices not connected to the same managed network switch. It allows us to separate a single physical network into many virtual networks, allowing devices to communicate as if they were on other physical networks.

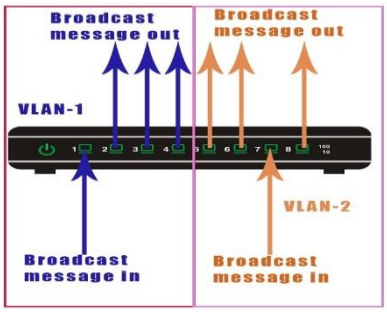
1.2. VLANs are mostly used in switches to define independent broadcast domains at Layer 2 of the network architecture.

1.3. VLANs can be configured station wise and are basically a collection of the same type of devices spread over a Railway Station. Designed to interact with each other through data links as they share the similar physical locations in the CCTV Network. VLANs behave like an independent LANs and are represented by numbers which are called VLAN ID, which are different and unique.

1.4. A VLAN is a switch-only feature. It allows us to define ports that share broadcast messages.

1.5. If two switch ports belong to different VLANs, they do not share broadcast messages. If two ports belong to the same VLAN, they share broadcast messages.

1.6. An example - Two VLANs: VLAN-1 and VLAN-2 on a switch.



Port-1 to 4 to VLAN-1 and Port-5 to 8 to VLAN-2.
After this, ports 1, 2, 3, and 4 will share broadcast in VLAN-1 and ports 5, 6, 7, and 8 will share broadcast in VLAN-2.

1.7. **Types of VLAN**

1.7.1. **VLAN for CCTV network are both Port-based & MAC-Based:**

1.7.1.1. **Port-based VLAN** − VLAN membership is decided by the physical switch ports to which devices are connected. Each port is assigned to a certain VLAN, and all devices connecting to that port are members of that VLAN.

1.7.1.2. **MAC-based VLAN** − The MAC (Media Access Control) address of devices determines VLAN membership. Administrators define MAC addresses and provide VLAN memberships.

1.8. **Advantages of VLANs**

1.8.1. **Security** − By segregating traffic within VLANs, VLANs improve network security. Unless specifically permitted, devices in one VLAN cannot communicate with devices in another VLAN. This segmentation helps to control potential security breaches and the scope of network attacks.

1.8.2. **Performance and Efficiency** − Broadcast traffic is contained within each VLAN when a network splits into VLANs, reducing network congestion and boosting performance. VLANs additionally allow more efficient use of network resources by grouping devices based on their purpose, department, or security requirements.

1.8.3. **Simplified Network Management** − VLANs make network management simple by grouping devices logically. Even within a shared physical network architecture, network administrators can establish VLAN-specific parameters, apply security policies, and operate VLANs individually.

1.9. **Use of Management VLAN**

1.9.1. A management virtual local area network (VLAN) is a much smaller network that is contained within your regular network.

1.9.2. The primary benefit of using a management VLAN is improved network security. When all management traffic is on a separate VLAN, it is much harder for unauthorized users to make changes to your network or monitor network traffic.

1.9.3. Another potential benefit is that a management VLAN can help you minimize the impact of a broadcast storm on other VLANs by giving you a separate path to access your network.

1.9.4. Note: Using a management VLAN is not a substitute for physical security. It is recommended that all networking devices (except cameras) should be kept in a secure location with restricted access.

Technical Advisory Note (TAN)			
Subject	Comprehensive Security Guidelines for CCTV Network.		
Doc. No.	STT/TAN/CCTV/2024	Version – 1.0	Date – 24.04.2024

1.10. VLAN Tagging

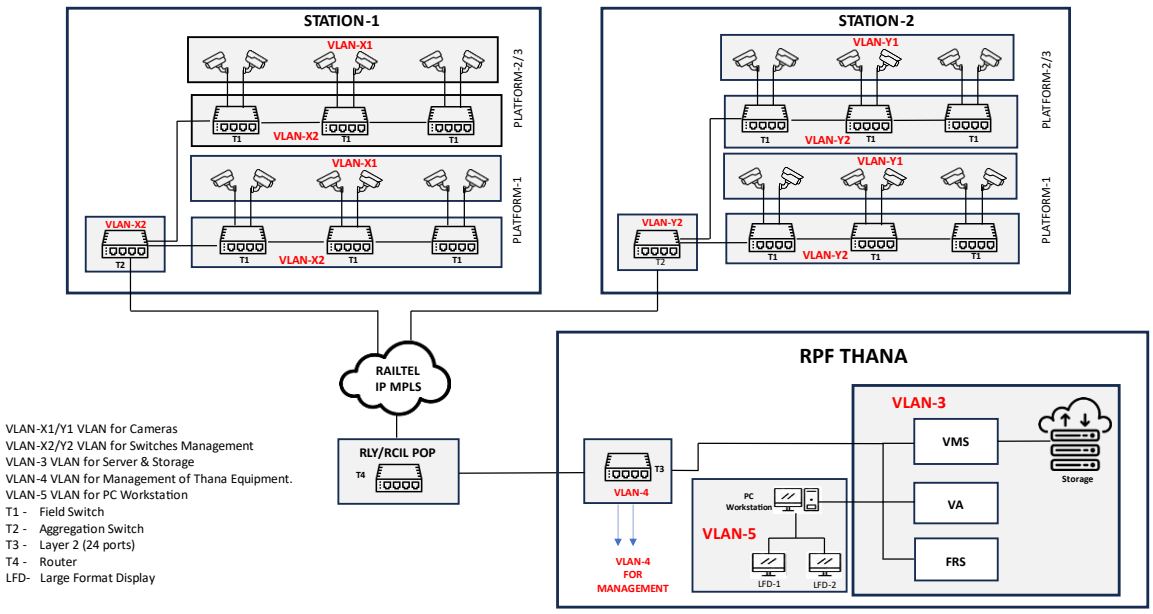
1.10.1. When transferring VLAN traffic over network links, especially in VLAN trunking circumstances, VLAN tagging is used. It adds a VLAN tag or VLAN identifier (VLAN ID) to the Ethernet frame to indicate which VLAN the frame belongs to. This allows switches and other networking devices to accurately detect and handle VLAN traffic, ensuring that frames are routed to the relevant VLANs.

1.10.2. Multiple VLANs can be tagged on a single port of any switch.

1.11. VLANs used in CCTV Network

1.11.1. Following is a typical network diagram that shows VLANs for CCTV Network:

VLAN NETWORK DIAGRAM FOR VSS SYSTEM



1.11.2. Following four VLANs have been used:

1.	VLAN1	Cameras (/24- 256 IP addresses)
2.	VLAN2	Switch Management (/25- 128 IP addresses)
3.	VLAN3	Server & Storage (/28- 16 IP addresses)
4.	VLAN4	Management of Thana Equipment (NVR, Servers, Storage, UPS, Type-3 Switch etc.)
5.	VLAN5	PC Workstation

1.11.3. As PC Workstation is quite prone to Virus, malwares and other security hazards due to the use of USB based pen-drives for extracting required video footages by RPF, a separate VLAN should be created for PC Workstation.

1.11.4. In addition, separate subnet should be used for each type of VLAN at each station.

1.11.5. VLAN-IDs plan (station wise) for CCTV Network of IR shall prepare by Nominated Zonal Railways/ RailTel and same will be circulated to all Railways for better implementation of CCTV Project.

1.11.6. Centralized DHCP Server (1+1 High availability) to be setup for Static IP allocation to CCTV cameras and NVRs using DHCP options.

Technical Advisory Note (TAN)			
Subject	**Comprehensive Security Guidelines for CCTV Network.**		
Doc. No.	STT/TAN/CCTV/2024	Version – 1.0	Date – 24.04.2024

Annexure-B

1. Verification of firmware HASH Value from Security Audit Certificate/ Report by RDSO during Type Test and Acceptance Test:

1.1. The Security Audit certification/report contains HASH value of the tested firmware by the lab and it is mentioned on certification/report.

1.2. General example of the HASH value & Algorithm from certification/report:

2.2	Version No.		
		Firmware Version	V 5
		Chipset	AmbarellaCV28
		Hash (MD5)	6f3383ae08b3408b3490ceef53e08b34

1.3. OEM shall be asked to provide the certificate/report containing the HASH value of the firmware.

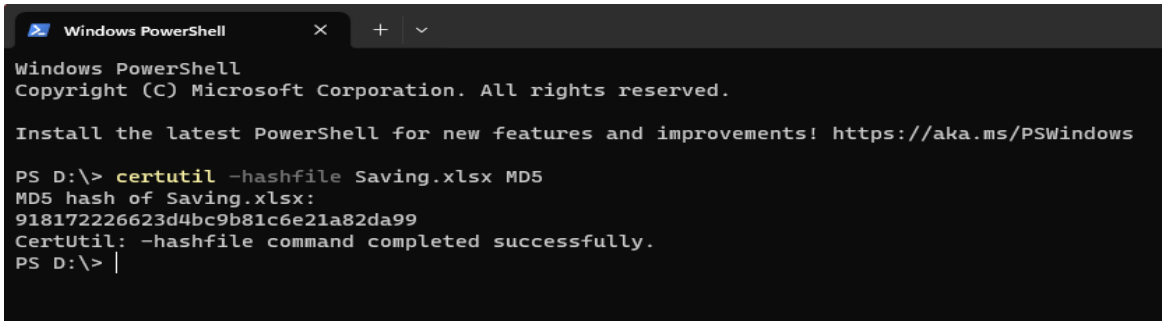
1.4. Now randomly selecting a camera from the supplied lot, OEM shall be asked to provide the firmware ".BIN" file from that randomly selected camera's (sample) flash memory.

1.5. In windows environment, OEM shall be asked to keep the ".BIN" file in a folder and open the "Command Prompt" in same folder and type the following command: **certutil -hashfile <".BIN" file name> <algorithm>**

1.6. Here **".BIN"** file name is the name given to the downloaded file and algorithm is as mentioned in the Security Audit report, it may be **SHA1** or **MD5**, etc.

1.7. The result of the **certutil** command will show the HASH value which should be the same as mentioned in the Security Audit certificate/ report in case when no changes is done afterwards in the firmware which was tested by the Security Auditing Lab.

1.8. General example of the **"certutil"** command:



1.9. **Note:** It may happen that the firmware file downloaded might be encrypted and the HASH value might not be the same as mentioned in the Security Audit certificate/ report.

1.10. In such cases, the OEM shall be asked to dump the file in plain text file with ".BIN" extension (or decrypt the file) and then OEM shall be asked to check the HASH value by the above-mentioned procedure.

2. Verification of System on Chip (SoC) of the IP based CCTV Camera by RDSO during Type Test and Acceptance Test:

2.1. The Security Audit certification/report contains SoC Name/Number of the tested hardware by the lab and it is mentioned on certification/report.

2.2. There can be two modes of verification for the SoC, namely, Physical Verification mode and Command-Line mode.

2.2.1. Physical Verification Mode:

2.2.1.1. The OEM shall be asked to open the randomly selected camera hardware and show the SoC.

2.2.1.2. The SoC shall have SoC Name/Number embossed on it.

2.2.1.3. Note the SoC Name/Number and verify from the Security Audit certification/report.

2.2.1.4. It should be same as mentioned on the Security Audit certification/report.

2.2.2. Command-Line Mode:

2.2.2.1. Every OEM has its own way to enter into Command-Line mode of the camera hardware.

2.2.2.2. Ask the OEM to connect the randomly selected camera on a PC or LAPTOP through the predefined communication port, e.g. UART / JTAG / Ethernet Port, etc.

2.2.2.3. Ask the OEM to open the camera information in windows environment - Command Prompt.

2.2.2.4. Camera details shall be displayed on pressing ENTER key.

2.2.2.5. It shall display the SoC details as well.

2.2.2.6. It shall be noted and cross-verified from the Security Audit certificate/report.

2.2.2.7. **Note:** The origin (country) of SoC can also be verified from the Web using various websites, e.g. octopart.com, etc. which can show the details of the SoC, if available.

2.2.2.8. If the details are not available, then ask the OEM to provide the data-sheet of the SoC.

****