OT Cybersecurity for Indian Railways

Securing Signaling, Operations & Safety in the Digital Era

Organized By - RailTel Corporation of India Limited

Mode:Online training

Date - 9th October 2025

Time - 10:30 AM to 5:30 PM

Rs. 9,750+ 18% GST

OT Cybersecurity Framework – 5 Pillars

1. Network Security

Objective: Protect the integrity, availability, and segmentation of OT network environments.

- Key Controls:
  - Network segmentation (e.g., Purdue Model)
  - Firewalls and industrial demilitarized zones (IDMZ)
  - Protocol filtering (Modbus, DNP3, OPC, etc.)
  - Intrusion Detection/Prevention Systems (IDS/IPS)
  - Asset discovery and passive monitoring

2. SCADA and ICS Security

Objective: Secure Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) from unauthorized access, manipulation, and failure.

- Key Controls:
  - Hardened configurations for PLCs, RTUs, and HMIs
  - Patch management tailored to OT systems
  - Device authentication and access control
  - Secure remote access to control interfaces
  - Protocol-aware threat detection

3. Security Operations Center (SOC) for OT

Objective: E[illegible] continuous monitoring an[illegible] response ca[illegible]

- Key Capabilities:
  - OT-specific log collection and correlation (e.g., from historian systems, PLC logs)
  - Integration with IT SOC for visibility across IT/OT boundaries
  - Threat hunting and anomaly detection in OT traffic
  - OT-aware SIEM platforms and use cases

4. Incident Response (IR)

Objective: Develop and test OT-specific response capabilities to detect, contain, and recover from cyber incidents.

- Key Elements:
  - OT incident response playbooks (e.g., ransomware in SCADA)
  - IR team training with OT scenarios
  - Isolation and recovery procedures for control systems
  - Forensics in OT environments (without disrupting operations)
  - Tabletop and red team exercises with OT focus

5. Compliance and Governance

Objective: Align OT cybersecurity posture with regulatory, industry, and internal governance standards.

- Key Standards & Regulations:
  - IEC 62443 (Industrial Automation)
  - NIST 800-82 (ICS Security)
  - NERC CIP (Energy sector)
  - ISA/IEC 61511 (Functional safety in process industries)
  - ISO 27001/27019 with OT extensions

Compliance & Standards Overview

1. IEC 62443 – Industrial Automation & Control Systems (IACS) Security

- Developed by: International Electrotechnical Commission (IEC)
- Purpose: Establishes cybersecurity requirements for Industrial Automation and Control Systems

2. NCIIPC – National Critical Information Infrastructure Protection Centre (India)

- Established by: Government of India under Section 70A of the IT Act, 2000
- Purpose: To protect Critical Information Infrastructure (CII) in India.
- Applicable to: Sectors like Power, Telecom, Finance, Transport, Government, and Strategic/Public Enterprises

3. Kavach – Cybersecurity Initiative (India)

- Meaning of Kavach: "Armor" or "Shield" in Hindi
- Purpose: Security product/initiative by Indian government for real-time cyber threat monitoring and mitigation
- Context-Dependent: There are multiple uses of the name "Kavach" in different cybersecurity/security programs.

Passenger Experience

- Comfortable, modern coaches
- Smart apps for real-time updates
- Enhanced cleanliness and catering

Integration & Compliance StrategyIEC 62443

Standard/Framework	Domain	Focus Area	Recommended For
IEC 62443	Industrial Systems	ICS/OT Cybersecurity	Manufacturers, Critical Infrastructure
NCIIPC	National Critical Infrastructure	Protection & Policy	Govt and Strategic Sector Entities
Kavach	Email/Cybersecurity Tools	Authentication, Threat Response	Govt Email Users, Cyber Defense Systems

Case Study: Cyber Protection of a Railway Signaling System

In this case study, we explore the cyber protection of a Railway Signaling System, a critical component of modern railway infrastructure. The system controls train movements and ensures safety by signaling trains and preventing collisions. Given the increasing complexity of signaling systems and their integration with IT networks, cybersecurity plays a vital role in preventing disruptions, accidents, and even national security threats.

1. System Description

The railway signaling system is responsible for the control, monitoring, and operation of trains. The system includes various components such as:

- Trackside signaling equipment (signals, points, and interlocking systems)
- Control centers (centralized or distributed)
- Train communication systems (real-time position reporting)
- Railway network monitoring systems (e.g., SCADA systems)
- Automated systems (for controlling train speeds, schedules, and routes)

2. Threat Landscape

Cyber threats to the railway signaling system can include:

- Cyberattacks (e.g., hacking attempts on control systems, ransomware)
- Data tampering (e.g., altering train schedules, signaling data)
- Denial-of-Service (DoS) attacks (targeting system availability)
- Insider threats (e.g., unauthorized access from staff)
- Supply chain vulnerabilities (e.g., compromised software or hardware components)

3. Cybersecurity Framework Applied

To mitigate these threats, the railway signaling system is protected using a combination of various standards and best practices. In this case study, we implement IEC 62443, NCIIPC guidelines, and Kavach (where applicable).

a. IEC 62443 – Industrial Cybersecurity for Operational Technology (OT)

b. NCIIPC Guidelines – Critical Infrastructure Protection

c. Kavach – Cybersecurity Authentication & Monitoring Tools

---

4. Risk Mitigation Strategy

a. Network Segmentation and Isolation

b. Secure Software & Hardware

c. Incident Response Plan

d. Employee Awareness and Training

---

5. Example of Cyberattack Simulation and Response

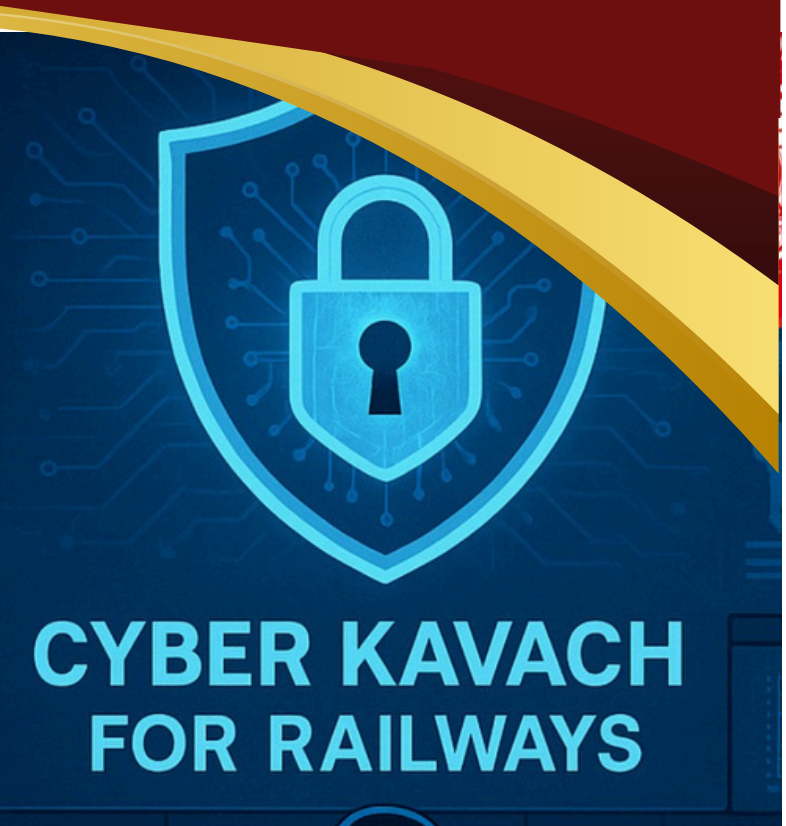
Scenario:

A ransomware attack attempts to lock critical signaling data, preventing communication between the control center and trackside devices.

Steps Taken:

1. **Detection:** The IDS identifies abnormal activity in the network, flagging encrypted data transfers to unknown locations.
2. **Containment**: The affected servers are isolated from the network, and control is shifted to backup systems.
3. **Recovery**: The system is restored from secure backups, and the ransomware is removed from the environment.
4. **Forensics**: The IRT analyzes the attack vector, discovering it originated from a phishing email targeting an operator.
5. **Preventive Measures:** Additional layers of email filtering and user authentication (multi-factor authentication) are implemented to prevent future

Securing the Future of Indian Railways



Contact Us

Mo.- +91 98111 13345
+91 9818636895

Coe@railtelindia.com

RailTel Corporation of India Limited
railtelindia.in

RailTel Corporation of India Limited
,Plate-A, 6th Floor, Office Block
Tower-2, East Kidwai Nagar,New Delhi-
110023

Bank details for Direct Bank Transfer
Account Name: RailTel Corporation of India Limited
Account Number: 340601110050003
Bank Name: Union Bank of India IFSC: UBIN0534064

Online registration and Payment
www.railedutech.com

Scan and pay