DATACOM INDUSTRY ASSOCIATION

Wi-Fi in Railways

Use Cases and Cybersecurity Aspects

DIA Railway Working Group

© 2026 Datacom Industry Association (DIA).
All rights reserved. Reproduction or distribution, in whole or in part, is permitted with attribution

Executive Summary

Rail mobility is a vital pillar for sustainable transport. Digitalization has emerged as a key catalyst to increase rail operations and to accelerate the transition to green transport. Deploying modern communication networks unlocks deep operational efficiencies and elevates the passenger Quality of Experience (QoE). Wi-Fi high-speed broadband connectivity is the foundational layer to drive such operational and passenger advancements.

Commercial Wi-Fi standards have evolved into a high-capacity technology capable of supporting intense data demands and the requirements of the innovative bandwidth-intensive railway applications, including artificial intelligence model training and augmented reality systems.

Beyond raw speed, newer Wi-Fi generations, such as Wi-Fi 7, introduce a major paradigm shift through Integrated Sensing and Communication (ISAC). The network analyzes signal propagation to recognize physical movement, human presence, and environmental anomalies without requiring secondary physical sensors.

Operationally, the industry is shifting away from maintaining physically separate Wi-Fi networks for distinct railway services. Instead, modern architectures utilize a unified physical infrastructure that is logically segmented through robust network slicing and Quality of Service (QoS) frameworks. This converged Wi-Fi infrastructure serves as a digital backbone to aggregate On-board control data, to convey connectivity to passengers, and to enable sensing applications.

As railway networks consolidate, the expanding digital footprint increases the potential impact of cybersecurity failures. Because wireless signals inherently extend beyond the physical boundaries of rolling stock and stations, physical isolation is impossible. A defense-in-depth security philosophy has to be considered, utilizing layered technical controls and rigorous lifecycle governance rather than relying solely on protocol compliance.

Architecturally, network convergence decisions must be governed by structured risk assessments. In alignment with the IEC 62443 framework, industrial systems should be partitioned into distinct security zones connected by tightly controlled conduits. Sharing physical infrastructure is appropriate only for non-safety-critical operational data, such as passenger information updates or non-critical diagnostic logs.

Finally, security governance must extend to maintenance environments. Stationary or shut-down trains running background diagnostic links face unique proximity threats from contractors and unauthorized personnel. Maintenance yards must enforce mutual device authentication, maintain audit logs, apply strict session time limits, and keep all diagnostic interfaces entirely isolated from general depot or passenger networks.

Table of Contents

1 Introduction 6

2 Wi-Fi Generations and Technical Characteristics 7

3 Current Wi-Fi Adoption by Railways 9

4 Enhanced and Innovative Wi-Fi Use Cases in Railways 10

4.1 Seamless, high-quality passenger connectivity 10

4.2 On-board train communication and services 10

4.3 Station communication and services 11

4.4 Operations at the shunting yard, depot, & maintenance centre 11

4.5 Wi-Fi Sensing for advanced applications 12

4.6 Evolution of wireless communication for signalling 12

5 Cybersecurity Analysis 13

5.1 Wi-Fi cybersecurity and secure infrastructure sharing 13

5.2 Detection of network anomalies 15

5.3 Secure one-way transfer of operational information 16

5.4 Security monitoring of trains, stations & maintenance facilities 17

6 Conclusion and Future Actions 19

References 20

List of Contributors

Name	Affiliation
Daniele Bozzolo	DBG Consulting
Davide Amato	Sadel
Martin Reed	University of Essex
Paolo Volpato	Huawei

List of Abbreviations

AI – Artificial Intelligence
AP – Access Point
AR – Augmented Reality
CCTV – Closed-circuit television
CSI – Channel State Information
DMR – Digital Mobile Radio
EU – European Union
EVC – European Vital Computer
FRMCS – Future Railway Mobile Communication System
GSM-R – Global System for Mobile Communications – Railway
KRACK – Key Reinstallation Attack
IEEE – Electrical and Electronics Engineers
ISAC – Integrated Sensing and Communication
IT – Information Technology
ML – Machine Learning
MLO – Multi-Link Operation
OT – Operational Technology
PIS – Passenger Information Services
QoE – Quality of Experience
QoS – Quality of Service
RU – Railway Undertakings
TCN – Train Communication Network
VR – Virtual Reality
WPA – Wi-Fi Protected Access 2

1 Introduction

The European Union (EU) considers rail mobility an economically, ecologically, and socially effective means of achieving greener [1]. Factors such as increased punctuality, high service reliability, and competitive pricing typically influence the choice of rail as the preferred mode of transport for passengers and freight.

Digitalisation unlocks new opportunities to improve rail operational efficiency [2]. Digitalisation also offers the potential to enhance the passenger Quality of Experience (QoE), a key catalyst for shifting public habits towards a green transition in transport.

The scope of this paper is to evaluate the technical merits of Wi-Fi-based high-speed broadband connectivity in supporting operational efficiency and driving passenger preference for rail transport.

Modern Wi-Fi product generations integrate high-speed connectivity with advanced functionalities, such as sensing. Integrated Sensing and Communication (ISAC) enhances safety and security across day-to-day rail operations and passenger environments.

The remainder of this paper is structured as follows: Section 2 compares the technical characteristics of current Wi-Fi standards. Section 3 examines typical Wi-Fi deployments both on-board trains and within railway stations. Section 4 outlines advanced scenarios leveraging Wi-Fi connectivity and sensing to improve passenger QoE, optimise operations, and heighten security. Finally, Section 5 delivers a comprehensive cybersecurity analysis of these use cases, addressing primary technical security concerns.

2 Wi-Fi Generations and Technical Characteristics

Wi-Fi systems are categorized into families, which are commonly referred to as generations. The Wi-Fi Alliance [3] holds the Wi-Fi trademark and defines the standards for system interoperability. On the technical side, the Institute of Electrical and Electronics Engineers (IEEE) establishes the technical characteristics of these standards within the IEEE 802.11 specification family [4]. Table 1 outlines the core technical specifications of standard, off-the-shelf Wi-Fi generations.

Wi-Fi generation	**Wi-Fi 4**	**Wi-Fi 5**	**Wi-Fi 6**	**Wi-Fi 6E**	**Wi-Fi 7**
IEEE standard	802.11n	802.11ac	802.11ax		802.11be
Publication (year)	2009	2013	2019	2021	2024
Max data rate	0.6 Gbps	3.5 Gbps	9.6 Gbps		40 Gbps
Operating frequencies	2.4, 5 GHz	5 GHz	2.4, 5 GHz	2.4, 5, 6 GHz	
Channel spacing	20, 40 MHz	20, 40, 80, 160 MHz			20, 40, 80, 160, 320 MHz
Channel bonding	40 MHz	160 MHz			320 MHz
Sensing	No				Yes
Typical use	Basic connectivity	Connectivity in public/city areas	Smart homes, IoT, enterprise	Streaming, gaming	Low latency, bandwidth intensive (AR/VR, AI)

Table 1 – Characteristics of the Wi-Fi generations currently on the market

Over the years, Wi-Fi systems have evolved to deliver multi-gigabit speeds and enhanced spectrum efficiency. This evolution enables support for advanced applications that require ultra-low latency and high throughput, such as Augmented or Virtual Reality (AR/VR) and Artificial Intelligence (AI) model training.

The standard has continuously advanced by introducing sophisticated new features. Recent Wi-Fi generations have extended operations into the 6 GHz band, supplementing the traditional 2.4 GHz and 5 GHz spectra. Additional spectrum allows networks to serve more users and high-demand applications simultaneously. Newer Wi-Fi generations support wider channel spacing and channel bonding — the bundling of multiple smaller channels

into a single, larger channel — both of which significantly increase user bandwidth.

Beyond high-speed connectivity, Wi-Fi 7 introduces integrated sensing capabilities. Wi-Fi sensing analyses wireless signal propagation using advanced algorithms to detect motion, human presence, or hidden physical threats within a coverage area, thereby enhancing security and safety.

Modern Wi-Fi generations maintain backward compatibility with legacy systems. Older devices can still connect to modern Wi-Fi networks, though their performance remains constrained by the speeds, capabilities, and older security mechanisms of their respective generations.

3 Current Wi-Fi Adoption by Railways

The importance of Wi-Fi connectivity in the railway sector has grown progressively, establishing it as a critical asset for enhancing both operational efficiency and customer experience.

For passengers, high-speed and long-distance trains are increasingly equipped with Wi-Fi Access Points (APs) to provide On-board Internet connectivity and access to infotainment systems, such as Passenger Information Services (PIS) and dedicated travel portals.

The quality and stability of the backhaul uplink between the train and the mobile network provider depend heavily on factors such as trackside radio coverage, link bandwidth, and the specific technology deployed (e.g., 4G, 5G, or satellite).

In addition, public Wi-Fi is widely offered to customers in large and medium-sized stations as a core component of smart-city infrastructure. Station-based Wi-Fi grants passengers immediate access to the same digital connectivity and infotainment platforms available on-board. To streamline this transition, several Railway Undertakings (RUs) offer a unified digital experience, allowing passengers to hand over seamlessly from station Wi-Fi to the on-train network without the need to re-authenticate.

Beyond passenger services, Wi-Fi serves as a foundational layer for rail operations and rolling stock management. On-board trains, Wi-Fi networks aggregate and dispatch telemetry and control signals from multiple devices, sensors, and sub-systems. Furthermore, high-bandwidth Wi-Fi enables real-time streaming from on-board CCTV cameras, directly enhancing passenger safety. Within stations, Wi-Fi networks connect critical rail Information Technology (IT) assets, including digital ticketing systems, information displays, and dynamic digital advertising. Wi-Fi connectivity is particularly valuable in shunting yards, depots, and maintenance centres; it allows engineering teams to interface with train systems and enables remote, unmanned train monitoring platforms to sync with ground applications. This offloads large volumes of diagnostic data rapidly, avoiding the data constraints and costs of public cellular networks.

Due to stringent security requirements, passenger and operational traffic are traditionally isolated on physically separate Wi-Fi networks, both On-board and at stations. However, the current industry trend is moving towards convergence, integrating disparate applications onto a single physical network infrastructure while segmenting services logically. This architecture ensures that each application group is strictly segregated using robust network slicing and quality-of-service (QoS) frameworks, guaranteeing distinct security treatments and performance tiers.

4 Enhanced and Innovative Wi-Fi Use Cases in Railways

This section explores different use cases where Wi-Fi connectivity and integrated sensing can enhance passenger QoE, optimise rail operations, and streamline support activities for railway personnel. The core applications include:

1. Seamless, high-quality passenger connectivity.
2. On-board train communication and services.
3. Station communication and services.
4. Operations at the shunting yard, depot, and maintenance centre.
5. Wi-Fi Sensing for advanced applications.
6. Evolution of wireless communication for signalling.

4.1 Seamless, high-quality passenger connectivity

The objective of this use case is to provide a passenger with a high-speed Wi-Fi connection that allows seamless coverage from the station to the train. A passenger connects to and authenticates at the station's Wi-Fi network. Connectivity seamlessly follows the passenger when moving on the train's Wi-Fi network, without any need to re-authenticate.

For this uninterrupted, seamless movement (handover), both networks broadcast the same SSID and share the same passwords. A Wi-Fi device handles the handover entirely in the background without dropping the connection: the device constantly monitors the signal strength of the Access Points (AP) of both networks. Before the device disconnects from the first AP, it pre-authenticates with the second AP. The device quietly swaps its radio connection to the stronger AP. The original IP address is also kept, so that the service connection is not lost.

For Wi-Fi 7 in particular, a device can take advantage of Multi-Link Operation (MLO), allowing data transmission across multiple frequency bands simultaneously (a combination of 2.4, 5, or 6 GHz) thus increasing the average user bandwidth and diminishing latency.

As previously highlighted, the bandwidth achievable during the travel depends on the uplink, which is independent from the On-board Wi-Fi.

4.2 On-board train communication and services

The digital systems installed on modern trains, including sensors, devices, personnel's handhelds, and passengers' information systems, are connected to a Train Communication Network (TCN) [5], either wired or wireless, which enables the exchange of data between different vehicles of a train. The TCN is often physically separated from the passengers' Wi-Fi network due to security reasons.

The adoption of newer Wi-Fi generations characterized by advanced networking functions, allows the integration of the two physical networks into a single one with configuration of dedicated virtual networks for traffic segregation. To this extent, a Wi-Fi 7 functionality

may prove effective in the integration of the two networks, namely the transmission security at the physical layer. Radio signal is scrambled over the air interface by the Wi-Fi AP, which superimposes random interference noise on the radio waves transmitted a few centimetres far from the legitimate receiving terminal. Packets are thus disrupted at the physical layer, making impossible to trace and decode them by an attacker.

Enhanced physical security is critical for cases such as:

- On-board multimedia communication between railway staff: drivers, guards/conductors, technical personnel can securely communicate through the On-board train network (in case of accidents they may also use the passengers' network).
- On-board data exchange to terminals and control systems: train systems communicate to each other via Wi-Fi to exchange real-time information and to collect status and logs. Critical signalling and safety-related systems can securely communicate with the European Vital Computer (EVC), protected from eaves dropping or men in the middle attacks.
- Video Surveillance/CCTV cameras: both internal and external cameras monitor the train and surrounding environment. Video streams are securely transmitted to storage devices for recording and subsequent viewing.

4.3 Station communication and services

Rail station Wi-Fi networks are used by railway operators for different purposes, including operational and safety functions. Typically, these networks act as a digital backbone to connect ticketing systems, interactive kiosks, real-time high-definition CCTV feeds, PIS, and emergency broadcast systems.

In addition, when a train enters the coverage area of a Wi-Fi network at a station, it may connect to perform operational tasks (e.g., upload/download of trip data and logs to/from the ground control room).

The already mentioned characteristics of Wi-Fi 7 enable a fast and secure exchange of both IT and Operational Technology (OT) data between the relevant system.

In addition, Wi-Fi sensing enables advanced functions as described in section 4.5.

4.4 Operations at the shunting yard, depot, & maintenance centre

When at a depot, the train's systems and the rail personnel connect to the local communications network to perform management tasks and to communicate. Train On-board systems can exchange data with ground systems, including status of equipment, sensors log, journey data, train composition and braking characteristics, maintenance information. Data exchange is bidirectional, from train to ground and the other way around. Maintenance personnel can connect to both the On-board and the depot communication network via Wi-Fi. Wi-Fi provides wider broadband connectivity at lower latency allowing completion of heavy-duty management tasks (e.g., the download of CCTV recordings or upload of infotainment content and movies) in seconds.

4.5 Wi-Fi Sensing for advanced applications

Wi-Fi sensing (IEEE 802.11bf) [14] is a key functionality of Wi-Fi 7. In its essence, Wi-Fi sensing analyses how the Wi-Fi signals sent by Wi-Fi devices (e.g. APs, users' devices) behave when propagating in a certain environment, such as a train or a station hall. Intelligent algorithms analyse the resulting signals and recognize if anomalies occur caused, for example, by erratic human behaviour or a person falling to the floor due to illness, triggering an immediate intervention of first-aid personnel.

Wi-Fi sensing can be used to complement typical On-board, station- or yard-related security functions. While a security video camera operates in line-of-sight, Wi-Fi sensing processes the radio signal in non-line-of-sight. Wi-Fi Channel State Information (CSI) is continuously monitored by an AP. When a CSI amplitude change is detected, as an example due to object movement, radio signal propagation is affected. Proper processing of this signal changes, for example based on AI or Machine Learning (ML) algorithms can detect the unwanted presence of people On-board or in a closure even without the support of security cameras.

Thank to this capability, new applications can be developed, such as passengers' counting On-board a train (complementing the current systems typically deployed in proximity of the train doors) or at stations, seat or toilet occupancy, security-related behavioural patterns, first-emergency response as well as self-check of no person present on board when train is sent to depot.

Other possibilities include baggage tracking, e.g. the monitoring of the position of the baggage on a train so that in case an anomaly is detected (e.g. the distance between a passenger and a piece of luggage is deemed excessive for a determined time interval) a warning may be raised.

4.6 Evolution of wireless communication for signalling

Global System for Mobile Communications – Railway (GSM-R) and Digital Mobile Radio (DMR) are commonly used to carry low-bandwidth, mission-critical signalling.

The ability of Wi-Fi to provide wider broadband connectivity at lower latency makes it a fit for short railway lines where GSM-R is not economically convenient. Wi-Fi offers a good compromise between the technical requirements (e.g. coverage) and operational aspects (e.g., deployment cost). A number of Wi-Fi APs can be deployed along the track leveraging the already present cabling and electronics (e.g., to control the level crossings) and power facilities. The use of highly directional radios can compensate for the rapid signal weakening when moving to the edge a Wi-Fi cell. Worth noting, Wi-Fi can be combined with 5G in Future Railway Mobile Communications System (FRMCS) solutions. Research projects are currently exploring innovative deployment, use, and performance of Wi-Fi in such scenarios.

5 Cybersecurity Analysis

The increasing use of Wi-Fi for passenger services, railway operations, maintenance activities and sensing creates opportunities to consolidate infrastructure and provide new services. However, it also increases the potential impact of a cybersecurity failure. Railway Wi-Fi should therefore not be considered solely as a means of providing wireless connectivity. Its security architecture must account for the different levels of trust, criticality and safety consequence associated with passenger, business, operational and safety-related systems (6).

5.1 Wi-Fi cybersecurity and secure infrastructure sharing

Modern Wi-Fi security mechanisms provide authentication, confidentiality and integrity protection between a wireless device and an AP (6). Nevertheless, the security of a Wi-Fi network depends upon the complete implementation, including the security protocol selected, credential management, configuration of the APs and clients, software maintenance and the architecture of the network behind the wireless interface. General guidance for enterprise wireless networks therefore recommends considering the complete lifecycle of the wireless infrastructure, including configuration, monitoring, vulnerability management and periodic assessment (6).

Historical vulnerabilities demonstrate why compliance with a particular version of a wireless security protocol is not, by itself, sufficient. Just one of the many examples is the Key Reinstallation Attack (KRACK), disclosed in 2017 (7), exploited the handling of retransmitted messages during the WPA2 four-way handshake. A notable aspect of this vulnerability was that, although the four-way handshake itself had been formally shown to be secure, many contemporary implementations contained the same key-reinstallation flaw, allowing cryptographic keys to be reinstalled and security protections to be undermined.

Although KRACK is now a historical example, it is one of many vulnerabilities that have affected Wi-Fi implementations. Such examples demonstrate the need for particular caution when deploying Wi-Fi within critical systems. Unlike a wired network, the wireless transmission medium is inherently open and extends beyond the physical boundaries of the equipment, making physical isolation of the communication medium impossible. Security must therefore rely on correctly implemented technical controls and a defence-in-depth architecture. The KRACK example also demonstrates the importance of maintaining supported equipment, applying security updates promptly and avoiding dependence on any single security control (6).

Where possible, railway operational networks should use enterprise authentication with individual device or user identities rather than shared passwords. Authentication credentials should be managed according to the role and lifecycle of the device, allowing individual equipment to be revoked without changing credentials throughout the fleet. Protected management frames, secure administration interfaces, controlled configuration and continuous monitoring should also be used where supported. Legacy devices that cannot support current security mechanisms should be treated as a separate risk and placed within appropriately restricted network zones (9).

A significant architectural question is whether passenger connectivity and railway OT may

safely share the same physical Wi-Fi infrastructure. Sharing APs, cabling, antennas and management systems can reduce equipment, installation and maintenance costs. Modern enterprise Wi-Fi equipment can support multiple logically separated networks using different service identifiers, authentication policies, virtual networks and traffic-control rules. However, logical separation does not provide the same degree of independence as physically separate infrastructure. The networks may continue to share AP hardware, firmware, management systems, radio resources and supporting components. A vulnerability, configuration error, compromise of the common management platform or failure resulting in resource exhaustion could therefore affect more than one service.

Consequently, the acceptability of shared infrastructure should be determined by a risk assessment based upon the criticality and safety implications of the operational functions involved. The IEC 62443 approach of dividing an industrial system into security zones connected by controlled conduits provides a useful basis for this analysis. Systems with differing security requirements should be allocated to separate zones, with communication between them restricted to explicitly authorised flows [8], [9].

Sharing physical Wi-Fi infrastructure may be appropriate for non-safety-critical operational services where strong segregation, independent authentication, traffic filtering, capacity allocation and monitoring are provided. Examples may include passenger information updates, non-critical equipment monitoring or the transfer of maintenance records.

Physical separation does not necessarily require exclusive radio spectrum. Two independently managed Wi-Fi systems may continue to use the same unlicensed frequency bands and may therefore interfere with one another or compete for available radio capacity. Separate infrastructure can reduce the risk of cyber compromise propagating between networks, but cannot by itself guarantee communication availability.

Radio-frequency planning is particularly challenging for mobile railway systems because the wireless environment changes continuously as the train moves. A channel allocation that performs well at one location may encounter congestion, interference or different spectrum usage at another. Frequency planning must therefore consider the range of environments through which the train will pass, including stations, urban areas, depots and locations containing other railway or public wireless systems. In practice, static frequency allocation may need to be supplemented by dynamic channel selection, continuous interference monitoring and mechanisms for adapting to changing radio conditions.

Appropriate prioritisation and sufficient capacity are also required to ensure that lower-priority passenger traffic cannot adversely affect operational services. However, prioritisation cannot remove all risks arising from interference, congestion or deliberate radio-frequency disruption. Safety-related functions should therefore define safe and predictable behaviour when wireless communication is unavailable, delayed or degraded.

The same principles apply to trains within depots and maintenance yards. A train that is parked or nominally shut down may continue to operate wireless interfaces for diagnostics, software transfer, condition monitoring or maintenance. The presence of railway staff and contractors, together with the possibility of an unauthorised person approaching a train, creates a different threat environment from normal passenger operation. Wireless interfaces should expose only those services necessary for the current operational state, and access should require authenticated and authorised devices. Maintenance ac-

cess should be logged, time-limited where appropriate and separated from passenger or general-purpose depot networks.

5.2 Detection of network anomalies

Monitoring is an important component of defence in depth because preventative controls cannot be assumed to detect or prevent every attack. Railway Wi-Fi infrastructure can provide information about devices, authentication attempts, traffic patterns, radio conditions and network behaviour. Analysis of these data may help identify cybersecurity incidents, operational faults and changes in the wireless environment.

Wireless network monitoring may detect events such as repeated authentication failures, attempts to impersonate legitimate APs, unexpected APs or devices, unusual changes in signal characteristics, abnormal traffic volumes, unauthorised connections and communication between network zones that would not normally interact. Monitoring may also identify denial-of-service activity, radio interference or a compromised device generating traffic inconsistent with its expected role. Guidance for securing wireless local-area networks identifies continuous monitoring and periodic assessment as important components of WLAN security (6).

The monitoring approach should reflect the context of the network. Passenger networks are highly dynamic: large numbers of previously unseen devices may connect for short periods and generate diverse traffic. Behaviour that would be anomalous on an operational network may therefore be normal on a passenger network. Detection mechanisms should avoid relying solely on fixed device identities or simple traffic thresholds.

On an operational network, by contrast, equipment types, expected communication relationships and operating schedules may be relatively predictable. This may allow more restrictive allow-lists, communication profiles and behaviour-based detection. However, legitimate changes arising from maintenance activity, software updates, altered train composition or exceptional operating conditions must also be taken into account to avoid excessive false alarms.

Machine-learning techniques may assist with identifying unusual combinations of network behaviour, but their output should normally support rather than replace established security controls. Training data may not represent new operating conditions or previously unseen attacks, while an attacker may deliberately attempt to evade or influence a detection model. Alerts should therefore be correlated with other sources, such as infrastructure logs, equipment status, physical-access records and operational information, before an automated response is taken.

Recent work on Wi-Fi sensing extends the concept of anomaly detection beyond network traffic by using changes in radio-signal propagation to infer movement, occupancy and other physical events (15). These physical safety and security applications, together with their reliability, cybersecurity and privacy implications, are considered separately in Section 5.4.

5.3 Secure one-way transfer of operational information

Operational information may need to be made available to passenger-facing or business systems. Examples include train location, estimated arrival time, service disruption information, coach occupancy or the operational state required to generate PIS messages. At the same time, passenger-facing systems are exposed to a less trusted environment and should not provide an unintended route into train control or other operational systems.

Conventional network segregation can restrict communication between the operational and passenger domains using firewalls, access-control rules and application gateways. However, these controls normally remain capable of bidirectional communication and may be vulnerable to configuration errors, software defects or compromise. Where there is a strong requirement that information must leave an operational network but no communication may return, a unidirectional gateway, commonly referred to as a *data diode*, may be considered [10].

A data diode enforces one-way information transfer at the physical or hardware level. In the railway example, operational information could pass from the protected OT environment towards an intermediate service or the passenger information network, while traffic originating in the passenger network would be physically unable to reach the operational network through the same connection. Unidirectional gateways [10] are recognised as a defence-in-depth mechanism for exporting information from protected industrial environments [11], [12].

The use of a data diode is not transparent to all applications. Many commonly used transport protocols assume bidirectional communication. For example, TCP depends upon acknowledgements, retransmission and connection-management messages flowing in both directions. Simply blocking the reverse traffic may therefore prevent the application from operating correctly rather than creating a secure one-way service. A practical implementation typically requires trusted proxy services on either side of the diode. The transmitting proxy receives information from the operational application and transfers it through the one-way channel, while a receiving proxy reconstructs or republishes the information for use within the destination network [10].

The architecture should also consider data validation. A data diode prevents a network attack from travelling backwards across the one-way link, but it does not ensure that information leaving the operational system is correct, appropriate or free from malicious content. Information should be limited to the minimum required dataset, checked against an expected format and, where appropriate, authenticated so that the receiving system can verify its origin and integrity. The destination system should not automatically treat all data arriving through the diode as safe.

A unidirectional architecture is most suitable where the required information flow is genuinely one way. Where the operational application requires acknowledgements, requests, remote configuration or other return communication, alternative designs may be required. These may include a tightly controlled application gateway, a demilitarised zone or separate services for outward operational information and authorised inward commands. The security architecture should make the permitted information flows explicit rather than relying solely upon the apparent direction of an application-level connection. The UK National Cyber Security Centre provides a recent worked example addressing secure export

of data from an OT environment (12).

5.4 Security monitoring of trains, stations & maintenance facilities

Wi-Fi sensing is a new addition to the, primary, communication feature of Wi-Fi and, while in its early days, is being investigated for use in applications such as passenger counting (13). Wi-Fi sensing may also contribute to the physical security of trains, stations, yards and maintenance facilities (14). These environments present different operational conditions and should not be treated as a single sensing use case.

Within a station, Wi-Fi sensing could supplement CCTV, access control and staff observation by identifying unexpected occupation of restricted areas, unusual movement close to platform edges or railway infrastructure, crowd density and events consistent with a person falling or becoming incapacitated. Such information could be used to alert staff or direct existing surveillance systems towards an area requiring attention. The objective should normally be to provide additional situational awareness rather than to replace established safety systems.

Transport organisations are increasingly investigating the use of digital technologies to help identify potentially dangerous situations, including the presence of people in areas where there is a risk of deliberate or accidental entry onto the railway. Any use for detecting behaviour associated with a possible suicide or other personal crisis should be approached with particular care. A wireless sensing system cannot determine a person's intent and may incorrectly classify ordinary behaviour. Its output should therefore be expressed as an indication that may warrant human assessment rather than as a definitive identification of an individual or their intentions.

In maintenance yards and depots, sensing may help detect unauthorised entry, movement close to stored trains or the continuing presence of a person after an area or vehicle is believed to have been cleared. A parked train may retain stored energy, moving equipment or remotely activated systems even when it is not in passenger service. Detection of an unexpected person could therefore support both physical security and occupational safety. An alert might prevent remote activation, request confirmation that the train is clear or direct security personnel to investigate.

A similar function could be used on a train before it is moved into a depot or placed into an unattended state. Wi-Fi sensing could provide an additional check that no passenger or member of staff remains onboard. However, the consequences of a false negative may be significant. The sensing system should therefore supplement rather than automatically replace established train-clearance procedures unless its performance and safety integrity have been demonstrated for that application.

The sensing infrastructure itself must be protected. An attacker who could suppress, falsify or replay sensing information might conceal an intrusion or generate false alarms (15). Sensing devices, processing systems and alarm interfaces should therefore use authenticated communication, controlled administration, integrity protection and secure logging. Where sensing output affects an operational decision, the system should fail in a predictable manner and indicate when sensing coverage or confidence is insufficient.

Finally, the deployment should take account of privacy, transparency and data governance. Although Wi-Fi sensing may not produce recognisable video images, it can still reveal information about the presence, movement and behaviour of people. The absence of a conventional image does not mean that the data are inherently anonymous or without privacy implications. The intended purpose, retention period, access permissions and use of derived data should therefore be defined before deployment, with safeguards proportionate to the sensitivity and operational significance of the information (15).

6 Conclusion and Future Actions

The rapid evolution of Wi-Fi has transformed the technology from a standard consumer convenience into an asset for the modern railway sector. The latest Wi-Fi generations offer far more than simple passenger Internet access. By integrating ultra-low latency data transmission with capabilities like sensing, Wi-Fi networks act as a primary catalyst for driving operational efficiency, maximizing rolling stock utilization, and significantly elevating the passenger Quality of Experience (QoE).

Wi-Fi provides an optimal balance between high performance and low total cost of ownership. By leveraging existing trackside power and cabling infrastructure, operators can achieve high-capacity broadband connectivity on regional lines or within complex depot environments at a fraction of the capital expenditure required for standalone cellular rollouts. Furthermore, innovations like Multi-Link Operation (MLO) and directional antenna arrays guarantee that Wi-Fi can meet the rigorous bandwidth requirements of modern rail applications.

The physical convergence of public passenger traffic and critical operational technology onto shared physical infrastructure necessitates an in-depth approach to cybersecurity. While modern enterprise Wi-Fi supports advanced logical segmentation, network architects must implement strict technical controls to mitigate the expanded attack surface. Enforcing enterprise-grade 802.1X/EAP authentication, deploying hardware-enforced data diodes for one-way telemetry export, and isolating legacy devices are vital steps. Furthermore, it is fundamental to comply with international rail regulations related to safety-critical systems as defined by IEC 62443 specifications series.

By adopting modern Wi-Fi architectures, Railway Undertakings can successfully optimize day-to-day operations, safeguard critical assets, and deliver the seamless digital experience necessary to accelerate the global transition toward greener transport.

References

1. European Commission, COM(2020) 789 final, “Sustainable and Smart Mobility Strategy – putting European transport on track for the future”, December 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:5e601657-3b06-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

2. DIA Railway WG, Cyber security for the evolving FRMCS deployment in the European Railway Sector, December 2025

3. https://www.wi-fi.org/

4. https://www.ieee802.org/11/

5. EN IEC 61375-1:2026, “Electronic railway equipment - Train communication network (TCN) - Part 1: General architecture”, April 2026

6. M. Souppaya and K. Scarfone, Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153, February 2012

7. M. Vanhoef and F. Piessens, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2017

8. IEC 62443-3-2:2020, Security for Industrial Automation and Control Systems — Part 3-2: Security Risk Assessment for System Design

9. IEC 62443-3-3:2013, Industrial Communication Networks — Network and System Security — Part 3-3: System Security Requirements and Security Levels

10. V. Sundaravarathan et al., "Cross-Domain Solutions (CDS): A Comprehensive Survey," in IEEE Access, vol. 12, pp. 163551-163620, 2024

11. CISA/ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 2016

12. UK National Cyber Security Centre, Secure Connectivity: Operational Technology Data Export Example, 2026

13. H. Jiang, S. Chen, Z. Xiao, J. Hu, J. Liu and S. Dustdar, "Pa-Count: Passenger Counting in Vehicles Using Wi-Fi Signals," in IEEE Transactions on Mobile Computing, vol. 23, no. 4, pp. 2684-2697, April 2024

14. IEEE Std 802.11bf-2025, IEEE Standard for Information Technology — Wireless LAN Sensing

15. ETSI GR ISC 004 V1.1.1, Integrated Sensing and Communications: Security and Privacy, February 2026