Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26139-cd

Use Case Analysis of Quantum Key Distribution in Railway Systems

Katja Assaf[1]

Timo Ramsdorf[2]

Dirk Friedenberger[1]

Lukas Pirl[1]

Birgit Milius[2]

Andreas Polze[1]

1 : Hasso Plattner Institute, University of Potsdam, Germany. E-mail: firstname.lastname@hpi.de
2 : Technische Universität Berlin, Germany. E-mail: firstname.lastname@tu-berlin.de

With unprecedented computational capabilities, quantum computers pose a threat to IT security. Just like other domains, the railway domain is increasingly digitalized. Safety and efficiency are at stake. Quantum Key Distribution (QKD) is one approach to increase security in the post-quantum era. We identify 10 use cases for QKD in railway systems, involving interlockings, radio block centers, location cases, on-board units, infrastructure monitoring, dispatchers, drivers, conductors, platform supervisors, and remote operators. We characterize the use cases based on estimated demands for key exchange, confidentiality, integrity, availability, safety, and latency. Following the standard ETSI GS QKD 014, we consider integrations into the Transport Layer Security (TLS) protocol, which is also commonly used in railway applications. Especially for 5 use cases, we see a need for further research due to the mobility of communication endpoints, which may not even be capable of exchanging QKD keys directly.

Keywords: Railway, QKD, Command and Control Signalling (CCS), EULYNX, European Train Control System (ETCS).

1. Introduction

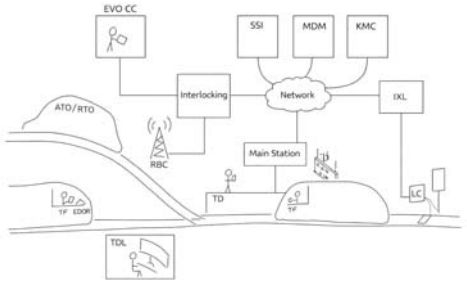

Figure 1. There are many potential use cases for QKD in railways. Some involve mobile endpoints.

The railway system is transforming into an increasingly digital system. An overview of the communication endpoints is shown in Figure 1. The foremost goal is to keep the system safe, i.e., to manage risks. In a digital system, where attackers can manipulate communication also over far distances, IT security is a necessity. Similar goals and restrictions are applicable in other transportation domains, such as automotive or aviation. The research project *SQuIRRL*[a] investigates the common requirements, designs, and develops a prototypical solution for promoting Quantum Key Distribution (QKD) in the transport sector.

We present use cases for the railway domain,

a. https://osm.hpi.de/squirrl/

where post-quantum security will be required in the future. The represented use cases are categorized according to their characteristics.

1.1. Background

Quantum key distribution (QKD) enables the secure exchange of cryptographic keys based on the principles of quantum mechanics. Advances in quantum optics and optical communication technology have facilitated the practical implementation of QKD systems (Elboukhari, Azizi, and Azizi 2009). To enable the distribution of quantum-mechanically secure keys, Quantum Key Distribution Networks (QKDNs) are required. Typical QKDNs rely on trusted nodes that serve as secure intermediate stations for key forwarding and storage. ETSI GS QKD 014 describes a lean, interoperable REST API for QKDNs that applications can use to securely retrieve cryptographic key material. Communication takes place via HTTPS with JSON between the Secure Application Entity (SAE) and Key Management Entity (KME) with mutual authentication. The standard promotes cross-vendor interoperability and a practical ecosystem for QKD applications.

1.2. Related Work

Apart from railway use cases, the *SQuIRRL* project also explores mobile use cases from the automotive and aviation domains. For the automotive domain (Ullrich et al. 2025), the use cases encompass encrypted data exchange between cars and charging stations. In this use case, the vehicle is not moving. The data to be secured includes, e.g., payment information. A second use case addresses software updates from Original Equipment Manufacturers (OEMs) for the Electronic Control Units (ECUs) in the cars. A characteristic of this use case is the chain of trust between a QKD endpoint and the actual application-layer communication endpoint. The aviation domain (Dautel, Lehmann, and Isidory 2025) also outlines two use cases. One use case is the integration of encryption via Transport Layer Security (TLS) into on-board avionics, adhering to an ARINC 2025 architecture. The other use case includes loading keys via QKD while on the ground and using the keys for air-to-ground communication via the Aeronautical Telecommunication Network (ATN). We focus on works relating to use cases with mobile endpoints.

A recent article (Aquina et al. 2025) contributes a comprehensive survey of real-world QKD use cases from academia and industry. Where sufficient information is available, the authors provide security evaluations that focus on comparison to post-quantum cryptography. Among the 14 sufficiently described use cases, there is a single case in which at least one communication endpoint is mobile. The online news release[b] describes an autonomous car being loaded with QKD keys using a fiber-optic cable. Subsequently, the keys were used for cryptography on a cellular connection. Since the article mentions telemetry and software updates, it can be assumed that the QKD-secured communication was used for these cases.

Tian et al. 2024 demonstrate a drone-based QKD system. The optical link is established free-field between a ground station and an airborne station carried by a drone. Both stations also establish a classical wireless channel non-QKD communication. The authors focused on the challenges of physical size, weight, and performance of the QKD hardware and the Acquisition, Pointing, and Tracking (APT) systems. A less intuitive achievement is a scheme for transmitting the polarization state. However, whether the key exchange rate would be sufficient for securing the drones' communication with the base station is not explicitly discussed. Additionally, free-field QKD and Unmanned Aerial Vehicles (UAVs) are outside the scope of the *SQuIRRL*

b. https://robotics.innopolis.university/news/universitet-innopolis-vnedril-v-bespilotniki-sistemu-kvantovogo-raspredeleniya-klyuchej-dlya-zashhity-ih-ot-vzloma/

project.

The work presented in Al-Mohammed et al. 2021 features a use case similar to our IXL-LC use case. The authors envision railway trackside infrastructure monitoring using Internet of Things (IoT) devices. Because of the typically resource-constrained hardware, computationally intensive tasks are performed on regional *IoT controllers*. These gateways are connected to a fiber-optical network, as often found along railway tracks. The QKD is intended to occur between the gateways and a remote server. The authors' focus is on the role of algorithms in detecting attackers in QKD. The focal point of the authors is the contribution of algorithms to detect the presence of attackers during QKD. Although the scenario described is in the railway context, the communication endpoints are stationary. We further do not expect the communication endpoints to be notably resource-constrained. Last but not least, we prefer to avoid transmitting QKD key material over post-quantum-insecure wireless links.

The use case presented in Nieto-Chaupis 2014 also considers mobile communication endpoints. The authors' main concern is uninterrupted QKD-secured communication between a client and multiple application servers. Although the use case considers a mobile communication endpoint, the actual QKD-secured communication happens between stationary communication endpoints only. Alike networking perspectives on QKD use cases can be found manifold in literature. For example, Mehic et al. 2020 examine network organization, routing, signaling, and simulation aspects.

2. Railway QKD Use Cases

The industry is working toward a command-and-control system with less trackside equipment, such as signals. Additionally, remote or automatic train operation (RTO/ATO) will mitigate worker scarcity. However, the systems require secure digital communication.

2.1. Signalling and Interlocking Technology Use Cases

Interlocking - Interlocking (IXL-IXL) Communication between adjacent interlocking systems serves the fundamental function of coordinating train movements across interlocking boundaries, ensuring safe and efficient route and line block operations. According to the *EULYNX* specification, an interlocking connection enables the electronic interlocking subsystem to send commands, process commands received from the adjacent system, transmit current statuses, and process statuses received from the neighbor system (*EULYNX* Consortium 2022, EuDoc7).

The *EULYNX* standard, the SCI-ILS interface provides a unified, standardized method for communication between adjacent interlockings. SCI-ILS uses Ethernet-based connections and the RaSTA protocol to securely transmit commands and status information, supporting both legacy interlockings via ILS adapters and new *EULYNX*-compliant systems. By standardizing the interface, SCI-ILS facilitates interoperability between different vendors and technologies while maintaining the essential functions of line block and route operation across interlocking boundaries (Lucas, Rothkehl, and Oetting 2023; *EULYNX* Consortium 2022, EuDoc7).

Interlocking - Location case (IXL-LC) An interlocking communicates with the object controllers in its interlocking area. Object controllers control field elements, such as signals, points, and level crossings, to ensure the safe operation of trains. The communication protocol between the object controller and the interlocking is the Rail Safe Transport Application (RaSTA), a UDP-based protocol that provides redundancy and real-time capabilities. As the RaSTA protocol does not offer security, future implementations as described by *EULYNX*, will wrap RaSTA messages into TLS.

The main security goal is authenticity and integrity, both of which are provided by TLS.

A forged message, e.g., a signal to halt or point to the left instead of the right, could interrupt railway operations. QKD is an option for providing the necessary key material to communication partners.

European Train Control System (RBC-OBU) The rollout of ERTMS/ETCS has already begun. The European Train Control System will ensure interoperability and reduce hardware and maintenance costs by eliminating the need for trackside equipment. Movement authorities can be transmitted via radio to the train instead of relying on trackside signals. Even now, the system relies on preshared keys, generated by a key management center and installed onboard manually. The main security goal is authenticity and integrity, both is provided by Euroradio, which provides a message authentication code, based on a railway specific variant of ISO9797-1. A forged message, e.g., a emergency stop, could interrupt railway operations. A forged movement authority could potentially be a first step in an attack chain with safety impact.

2.2. Operational Use Cases with Direct User Interface

Digital Command (DC (Std)) In rail operations, dispatchers transmit instructions to train drivers regarding the approval of movements, for example, including maximum speeds. This is usually done by controlling and monitoring signals, or, alternatively, by transmitting data to the driver's cab (e.g., in ETCS full-supervision mode). In both systems, technical malfunctions or special operating situations can occur for which no suitable signals are available. In these cases, written orders serve as a fallback for transmitting instructions. Dispatchers and train drivers use a standard form, the content of which is dictated by the dispatcher via train radio, written down by the train driver, and then repeated. As this process may only be carried out when the train is standing still, it is time-consuming and causes delays.

The digital command is a digital version of this procedure, in which the form is filled out electronically and made available to the train driver on a mobile device. This eliminates the need to dictate the command message. The current state of the art provides transmission via a cloud server and web-based access via HTTPS. Authorization of the dispatcher is currently done by internal employee accounts. Train drivers are authorized by a TAN transmitted via SMS (Kopitzki, Gütschow, and Norwig 2023).

Digital Command with Automatic Train Operation (DC (ATO)) A further development involves better leveraging the machine-readability of digital order messages. In the future, automatically operated trains (ATO) could execute some order messages without human intervention. This approach is a future scenario, but it is important given potential changes to protocols and security mechanisms, especially in key exchange.

Digital Departure Order (DDO/Zp9) After each passenger change on a train, a clearance procedure must be carried out before departure. Its aim is to ensure that the passenger change is complete and that all doors are properly closed. Today, clearance of short trains is often handled by the train driver, while longer trains are cleared by the train conductor or platform supervisor. In this case, the person responsible for clearance sends a departure order to the train driver upon successful clearance (in Germany, signal "Zp 9").

DB Fernverkehr uses a digital application for clearance processes. This application securely transmits the departure order to the train driver and controls the displays and loudspeaker announcements on the platform. Due to its direct relevance to safe train departure, the application can be classified as part of the critical infrastructure. From a technical perspective, the relevant endpoints of the system are both the passenger information system at the station and the mobile devices used by train conductors and drivers. In terms of QKD, this application is therefore similar to

the digital command described above.

Remote Train Operation (RTO) RTO refers to the remote control of railway vehicles, whereby a train driver controls the vehicle from a control center. The train driver is fully responsible for the journey. Autonomous driving functions are not included in this concept (Brandenburger and Stähli 2024).

There are safety-critical information flows in both directions between the control center and the vehicle. Operating commands must be reliably transmitted from the RTO workstation to the vehicle, while camera images and sensor data are transmitted in the opposite direction. Low latency is central to both information flows, as otherwise the vehicle's response times would increase. The integrity of the transmission is safety-critical, as manipulation could enable unauthorized access to vehicle control.

Another characteristic feature of this application is the specialized communication endpoints, including the vehicle control unit on the one hand and a highly specialized RTO operator workstation in the control center on the other. In addition, the continuous transmission of high-resolution image data requires a comparatively high bandwidth.

2.3. EULYNX Support Use Cases

***EULYNX* Standard Security Interface (SSI)** The *EULYNX* Standard Security Interface (SSI-XX), as defined in (*EULYNX* Consortium 2022, EuDoc117), provides services related to identities of assets and personnel, logging of events for further usage by a security event and incident management system (SIEM), backup services, and optionally a secure time. SSI-XX encompasses many protocols, including CMP for certificate management, HTTP and HTTPS for certificate revocation list distribution, and OPC UA and Syslog for logging.

***EULYNX* Diagnostic and Maintenance Interfaces (SDI-SMI)** The Standard Diagnostic Interface (SDI-XX) enables the collection, processing, and availability of diagnostic data from connected *EULYNX* subsystems, including event-based, preventive, and historical information. Similarly, the Standard Maintenance Interface (SMI-XX) supports maintenance and data management functions, such as the synchronous or asynchronous loading and activation of configuration data, software updates, and the initiation of maintenance procedures (EuDoc76,EuDoc77,EuDoc120). Both interfaces are implemented using an IP-based protocol stack, with OPC UA and binary encoding over TCP, employing a client-server model with secure, session-oriented communication. Additional SMI is using NTP over UDP for time synchronisation. These standardized protocols enable standardized, reliable access to diagnostic and maintenance data without impacting safety-critical operations (EuDoc16,EuDoc76,EuDoc77).

2.4. Other Use Cases

DBMAS DBMAS is a system within *Deutsche Bahn*'s infrastructure responsible for processing and coordinating a wide variety of fault and alarm messages (e.g., hot axle box detection and fire alarm systems). It is a complex system comprising server-side instances, field-side clients in the form of individual sensors, and client applications for the user interfaces of train dispatchers and fault clearance personnel. In addition to fault-clearance procedures, immediate train stopping may be required in safety-critical situations. The system architecture is based on OPC Unified Architecture, enabling standardized, interoperable communication between components[c]. A major challenge for possible QKD integration is likely to arise from the large number of manufacturers of the sensor technology. DBMAS integrity is critical, as emergency messages must be delivered reliably, and false alarms can trigger partial rail network shutdowns.

c. https://www.unified-automation.com/de/startseite/referenzen/case-studies/nachricht-detailansicht/opc-ua-im-system-dbmas-der-db-netz-ag.html

2.5. Use Cases Summary

Table 1 summarizes the use cases in the railway domain. Key charging describes whether the endpoints can be connected to the QKD network *permanently* or whether they need to rely on a *key charging station* for mobile devices. Key demand can be *low, medium or high*. For the RBC-OBU use case, for example, the onboard unit (OBU) on a train would need a maximum of 120 keys per day as currently the session length is 12 minutes on average. For use cases, such as IXL-IXL or IXL-LC, which secure a TLS connection sessions could last longer achieving the same level of security as TLS provides stronger security assurances.

Most messages are potentially safety-critical, integrity is a protection goal for all of our use cases, while confidentiality is only required in exceptional cases. $\sim$ indicates that while availability is desirable, an absence of the service would result in a fail safe state, halting trains, without any safety-critical impact.

Most services are safety-critical, meaning that a security breach can potentially harm humans. The *EULYNX* standard security interface (SSI), standard diagnostic interface (SDI) and standard maintenance interface (SMI) require confidentiality according to *EULYNX* (*EULYNX* Consortium 2022, EuDoc116). RTO transmits video material, and thus, confidentiality is also required. Latency is indicated as *low* if near real-time is required, *medium* if timing allows for roughly a second delay, and *high* if no hard restrictions are applied.

3. Railway QKD Use Case Taxonomy

To apply a QKD solution to a use case, the endpoints must be connected to the QKD network. Although stationary equipment can be permanently connected, the charging or maintenance window of mobile equipment must be long enough to allow sufficient time for key generation. Mobility of endpoints is the main characteristic as illustrated in Table 2. Other properties, such as safety-criticality or confidentiality, have only a limited influence on the QKD design. These properties primarily determine the recommended lifetime of the session key, as represented in the key demand column (Table 1). However, compared with today's data centers, the amount of data exchanged in the railway sector is very low.

3.1. Stationary Endpoint

Stationary endpoints can be directly connected to the QKD network. Thus, the architecture looks like a standard QKD-TLS solution as described in the ETSI 014 standard (ETSI ISG QKD 2019).

3.2. Mobile (ML1) Endpoint

A mobile endpoint, such as a train, cannot be permanently connected to the QKD network. However, there are maintenance phases when the train is in a workshop for several hours and could be connected to the system. Since trains are large enough, the QKD module can be installed on the mobile device. During the maintenance phase, keys are generated, which need to be stored for future use. The main difference from the stationary use case is the asynchronous key generation and communication (key usage) phases.

3.3. Mobile (ML2) Endpoint

As in ML1, these use cases include at least one mobile encryption endpoint; however, the endpoints are small devices that cannot currently integrate QKD modules, such as standard company smartphones or tablets. Key exchange for QKD on these connections can be achieved by installing the QKD module in a charging station. Mobile devices can be connected to the charging station to store new keys. Such a charging station can be positioned in service buildings so that staff often pass by it, while access by third parties is physically protected. As can be seen in Table 1, the key requirement in the use cases in this category is only low to medium, so that

Table 1. The table summarizes the use cases and their main characteristics.

Use Case	Main characteristic	Key Charging	Key Demand	C	I	A	safety	latency
IXL-IXL	Safety-critical communication, high availability	permanently	low	n	y	∼	y	medium
IXL-LC	Infrastructure and trackside equipment, permanently installed, safety critical protocol	permanently	low	n	y	∼	y	medium
RBC-OBU	Radio communication	charging station (train)	medium	n	y	∼	y	high
DC (Std)	Fallback orders, both endpoints are mobile devices	charging station (mobile device)	low	y	y	∼	y	high
DC (ATO)	Fallback orders, endpoints are indifferent between humans and machines	charging station (train/mobile device)	low	y	y	∼	y	high
DDO/Zp9	Mixed application with operational control and passenger information	charging station (mobile device)	medium	n	y	∼	y	medium
RTO	High bandwidth, low latency	mixed	high	y	y	∼	y	low
DBMAS	Alarm and fault messages, very large number of different device types	permanently	medium	n	y	y	y	medium
SSI	certificate management and security logging	permanently	medium	y	y	y	n	high
SDI / SMI	diagnostic and managment communication	permanently	low	y	y	y	n	high

enough keys can be loaded without affecting staff.

Table 2. The table summarizes how the use cases relate to the use case classification.

Type	Use Cases
Stationary	IXL-IXL, IXL-LC, DBMAS, SSI-XX, DBMAS, SSI, SDI/SMI,
ML1	RBC-OBU,
ML2	DC(Std), DC(ATO), DDO/Zp9, RTO.

4. Conclusion

Communication in railway systems needs to be post-quantum secure. We have explored use cases for QKD in Control-Command and Signalling (CCS) systems, among personnel, for monitoring, and for remote operation systems. A challenge is communication with mobile endpoints, such as trains. Complicating things, some endpoints cannot be equipped with QKD modules, such as smartphones. If QKD-equipped or not, both scenarios impose the challenge of requiring "key charging". In this challenge, we see potential to yield innovations compared to stationary-only domains.

Acknowledgement

The project on which this report is based is funded by the Federal Ministry of Research, Technology, and Space (BMFTR) under the funding codes `16KIS2166` (TUB) and `16KIS2165` (HPI). The responsibility for the content of this publication remains with the authors.

The authors would like to cordially thank all consortial partners of for the regular, benevolent, and fruitful cross-domain exchange.

Funded by: Bundesministerium für Forschung, Technologie und Raumfahrt

References

Aquina, Nick, Bruno Cimoli, Soumya Das, Kathrin Hövelmanns, Fiona Johanna Weber, Chigo Okonkwo, Simon Rommel, Boris Škorić, Idelfonso Tafur Monroy, and Sebastian Verschoor. 2025. "A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography." *EPJ Quantum Technology* 12 (1): 51.

ARINC. 2025. *ARINC 653P0-4:2025-12-01 — Avionics Application Software Standard Interface — Part 0: Overview of ARINC 653.* Technical report. December 1, 2025.

Brandenburger, Niels, and Mischa Stähli. 2024. "Remote Train Operation: Menschzentrierte Entwicklung einer Innovation." *ZEVrail – Zeitschrift für das gesamte System Bahn* 148 (11/12).

Dautel, Can André, Matthias Lehmann, and Edwin Isidory. 2025. "Introducing Quantum Key Distribution for Post-Quantum Secure Aircraft Maintenance and Communication Interfaces." In *2025 AIAA DATC/IEEE 44th Digital Avionics Systems Conference (DASC),* 1–7. IEEE.

Elboukhari, Mohamed, Mostafa Azizi, and Abdelmalek Azizi. 2009. "Integration of quantum key distribution in the TLS protocol." *IJCSNS* 9 (12): 21–28.

ETSI ISG QKD. 2019. *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.* ETSI Group Specification (GS) QKD 014. European Telecommunications Standards Institute (ETSI), February.

EULYNX Consortium. 2022. *Baseline Set 4.* Technical report. *EULYNX* Initiative.

Kopitzki, Matthias, Adrian–Leander Gütschow, and Björn Norwig. 2023. "Der Digitale Befehl: Prozessbeschleunigung und Arbeitserleichterung im Betrieb." *Deine Bahn* (February): 34–37.

Lucas, Julian, Markus Rothkehl, and Andreas Oetting. 2023. "Teil-Qualifizierung in der digitalen Leit- und Sicherungstechnik." *EI — Der Eisenbahningenieur* (January): 14–17.

Mehic, Miralem, Marcin Niemiec, Stefan Rass, Jiajun Ma, Momtchil Peev, Alejandro Aguado, Vicente Martin, Stefan Schauer, Andreas Poppe, Christoph Pacher, et al. 2020. "Quantum Key Distribution: A Networking Perspective." *ACM Computing Surveys (CSUR)* 53 (5): 1–41.

Al-Mohammed, Hasan Abbas, Afnan Al-Ali, Elias Yaacoub, Uvais Qidwai, Khalid Abualsaud, Stanisław Rzewuski, and Adam Flizikowski. 2021. "Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios." *IEEE Access* 9:136994–137004.

Nieto-Chaupis, Huber. 2014. "QoS evaluation for end user mobility for accessing classical and QKD networks." In *2014 IEEE Latin-America Conference on Communications (LATINCOM),* 1–4. IEEE.

Tian, Xiao-Hui, Ran Yang, Hua-Ying Liu, Pengfei Fan, Ji-Ning Zhang, Changsheng Gu, Mengwen Chen, Mingzhe Hu, Feng-Yu Lu, Chunxi Zhu, et al. 2024. "Experimental demonstration of drone-based quantum key distribution." *Physical Review Letters* 133 (20): 200801.

Ullrich, Henning, Dominik Bayerl, Thomas Hutzelmann, and Hans-Joachim Hof. 2025. "Application of Quantum Key Distribution in Intelligent Transport Systems." In *Proceedings of the 2nd Cyber Security in CarS Workshop,* 1–7.