Rail Security Expert Group

Legacy Network Protection

24E122
1A
17.10.2024

Modification history

Version	Date	Modification / Description	Editor
1A	17.10.2024	Initial Release published after internal and external (CER/EIM) review	Klas Andren, Jorge Gamelas, Christof Jungo, Oliver Lovric, Richard Poschinger, Patrick Rozijn, Max Schubert

Table of Contents

Table of Figures

1 Introduction

1.1 Scope

1.1.1.1 The purpose of this document is to provide guidance on protecting network communications for legacy systems. It provides mitigation measures for unprotected network communications using VPNs.

1.1.1.2 Legacy systems are not built according to IEC 62443

1.1.1.3 Legacy systems are not built according to the following standards:

- EULYNX BL4R1 or newer
- EU-Rail Security Specification (2025 or newer) and TSI versions based on these specifications

1.2 References

1.2.1.1 Subsets and EUG publication are referenced directly with their corresponding ID.

1.3 Other referenced documents:

[1] S. Bradner, “RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels,” Network Working Group, 1997.

[2] EU-Rail System Pillar CyberSecurity Group, Secure Communication Specification V0.90, 2024.

[3] D. Benjamin und C. Wood, „RFC 9258 - Importing External Pre-Shared Keys (PSKs) for TLS 1.3,“ 2022, Internet Engineering Task Force (IETF).

[4] Bundesamt für SIcherheit in der Informationstechnik, „Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2) - Version: 2024-1,“ 2024.

[5] CENELEC, „EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems,“ 2010.

[6] International Electrotechnical Commission, „IEC 62443-3-3 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels,“ 2013.

[7] EU-Rail System Pillar CyberSecurity Group, Shared Cybersecurity Services Specification V0.90, 2024.

[8] EU-Rail System Pillar CyberSecurity Group, Security Program Requirements Specification V0.90, 2024.

1.4 Abbreviations

IPsec ..... *Internet Protocol Security*
PSK ..... *Pre-Shared Key*
QoS ..... *Quality of Service*
SIEM ..... *Security Incident and Event Management*
TLS ..... *Transport Layer Security*
VPN ..... *Virtual Private Network*

ERTMS Abbreviations are listed in Subset-023

1.5 Authors

1.5.1.1 The Rail Security Expert Group (RSEG) consists of security experts of the following groups:

- ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
- EULYNX Security Cluster – Part of the EULYNX Initiative

1.5.1.2 The following members of the Rail Security Expert Group were involved in creating this document:

- ERTMS User Group (EUG) / EULYNX
  - Max Schubert
  - Richard Poschinger
- SBB
  - Oliver Lovric
  - Christof Jungo
- Trafikverket
  - Jorge Gamelas
  - Klas Andren
- NS
  - Patrick Rozijn
- SNCF
  - Nicolas Poyet

1.6 Applicability and Document Status

1.6.1.1 In order to ensure the usability for tender documents, this document is using classifications and requirement key words. This classification does not result in any binding requirements for members of the EUG or other involved parties. The documents will be updated in the future to be adapted to a changed threat landscape, updated standards, and newly developed security solutions.

1.7 Definition of Requirement Types

1.7.1.1 This document uses key words indicating requirement levels according to RFC 2119 [1]. Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified
O	Optional	not mandatory, must be as specified if implemented
I	Informative	included for clarification purposes only
R	Recommendation	included as recommendation

Texts without a tag do not constitute a requirement.

1.8 Definition of Terms

1.8.1.1 “VPN Components” are systems or software solutions providing cryptographic protection (integrity or confidentiality) of data in transit.

2 Architecture and Network Segmentation

2.1 Use Cases

2.1.1.1 Use Case Overview:

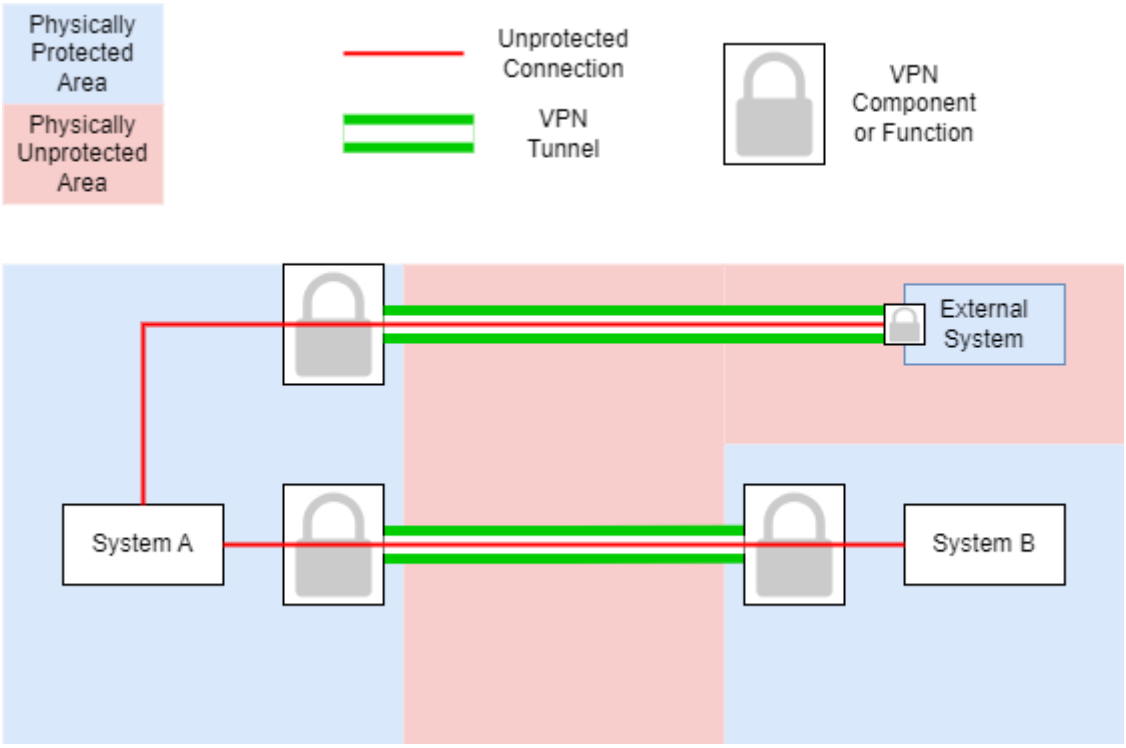

Figure 1: Use Case Overview

2.1.1.2 The following use cases are addressed in this document (see Figure 1) **(I)**

- Protection of point-to-point network traffic across untrusted networks [1] from (System A to System B as shown in Figure 1)
  - legacy safety systems
  - legacy non-safety systems
  - legacy high-availability systems
- Protecting remote connections (including maintenance access) to legacy systems
  (System A to External System as shown in Figure 1)

[1] Untrusted Networks: Category 2 and 3 networks according to EN 50159:2010

2.1.1.3 In addition to IP-based protocols, e.g. the following unprotected data transmission protocols exist in the railway domain. These protocols are not covered in this document. **(I)**

- Infrastructure
  - ISDN (without IP-based communication)
  - X.25
- On-Board
  - MVB
- CAN
- PROFIBUS

2.2 Maintaining safety/security-based network segmentation

2.2.1.1 The segmentation of VPN connections is shown in Figure 2 below. It shows three different logical connections (red, blue and pink) categorized as safety and non-safety related. White pipes indicate a separate physical connection on the system side and a physical connection used for the combined VPN traffic passing through the physically unprotected area. These three separate logical connections are separated using different VPN tunnels (green) in the same physical connection, maintaining the segmentation of connections according to the physical connection in the protected areas (blue). **(I)**

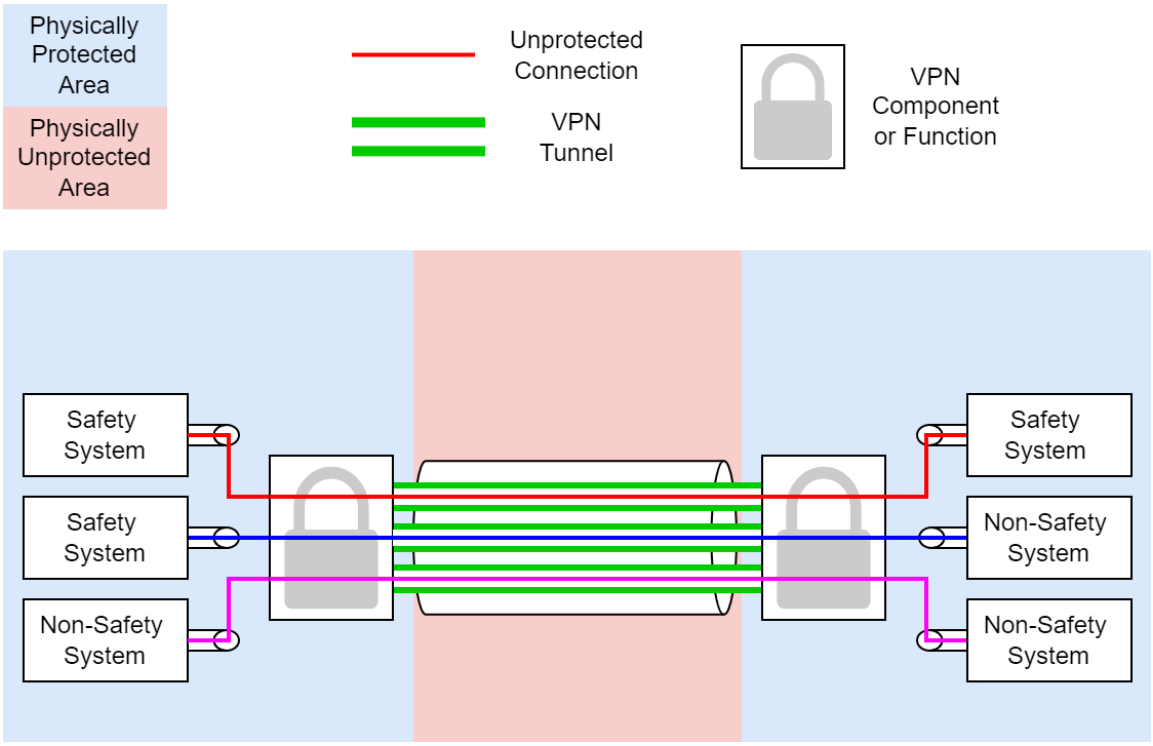

Figure 2: VPN Segmentation

2.2.1.2 The VPN component shall provide the same network segmentation as implemented in the existing installation. **(M)**

2.2.1.3 Maintaining the network segmentation results into establishing at least one VPN connection per physical or logical segmented connection. **(I)**

2.2.1.4 Physical network segmentation can also be established in the VPN segmentation by using one VPN component per segmented connection. **(I)**

2.2.1.5 Figure 3 shows that network segmentation also affects systems connected by multiple different physical connections. **(I)**

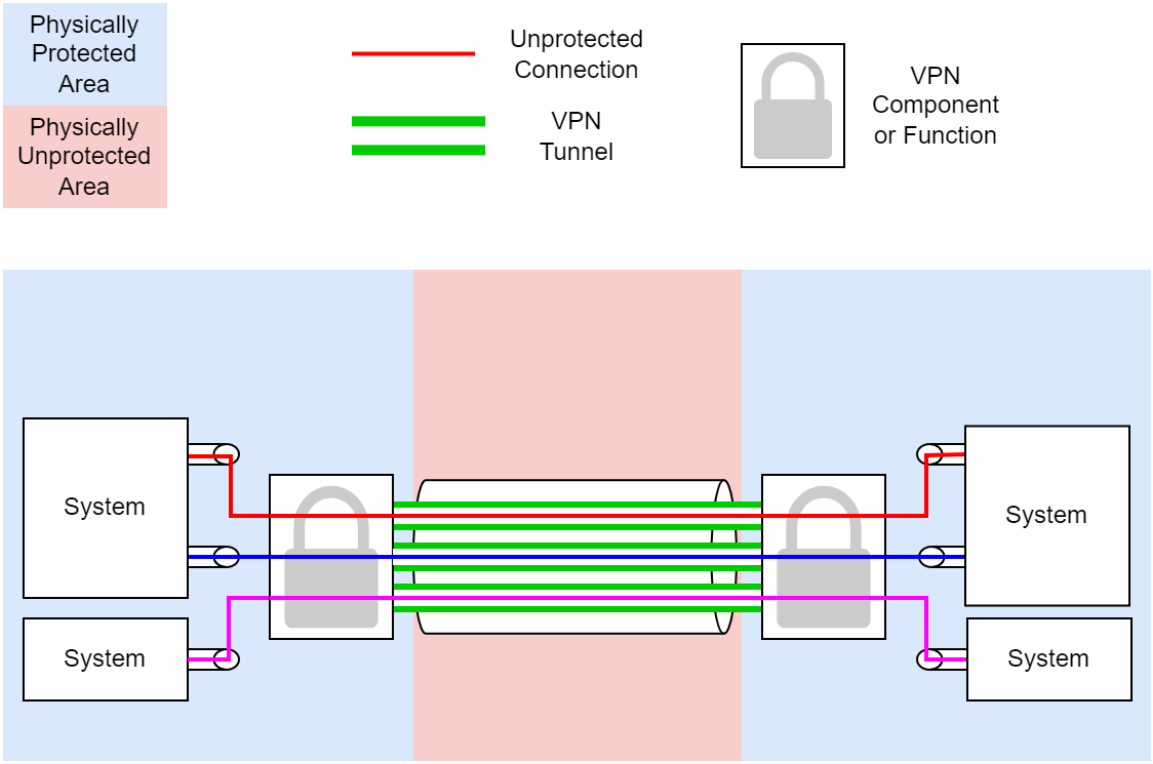

Figure 3: VPN Segmentation with Multiple Connections per System

2.3 Availability and Performance

2.3.1.1 The railway shall reassess the availability of the network including the VPN components. **(M)**

2.3.1.2 The railway shall ensure that the required availability is maintained using the VPN components**. (M)**

2.3.1.3 If the required availability cannot be satisfied using the VPN components, the availability may be provided by redundant VPN components and connection paths**.** This may include a multi-vendor strategy. **(I)**

2.3.1.4 The railway shall ensure that the required latency tolerance is maintained using the VPN components**. (M)**

2.3.1.5 The railway shall ensure that the VPN components provide the required bandwidth**. (M)**

3 Cryptographic Requirements

3.1 Encryption/Integrity Protection of network traffic

3.1.1.1 Protecting only the integrity of connections, rather than encrypting them, can provide the railway with the ability to inspect the network traffic without breaking the encryption. **(I)**

3.1.1.2 If the transmitted data has confidentiality protection requirements, the VPN component shall encrypt the network traffic. **(M)**

3.1.1.3 The railway shall perform a risk assessment addressing additional attack vectors (e.g., reconnaissance) to implement integrity only protection of network traffic. **(M)**

3.2 Protocols and Ciphers

3.2.1.1 The use of TLS for VPNs is not standardized. Therefore, protocols such as OpenVPN or proprietary protocols may be used, which may have different security implications. The following configurations can be used for TLS-based VPNs. **(I)**

3.2.2 TLS-PKI

3.2.2.1 The VPN component shall protect network traffic in accordance with the requirements of the EU-Rail Secure Communication Specification [2]. **(M)**

3.2.3 TLS-PSK

3.2.3.1 The VPN component shall protect network traffic according to the requirements of EU-Rail Secure Communication Specification [2] (Chapter 4.1 TLS Overall). **(M)**

3.2.3.2 The VPN component shall protect network traffic in accordance with RFC 9258 [2] (Importing External Pre-Shared Keys (PSKs) for TLS 1.3). **(M)**

3.2.3.3 The VPN component shall protect network traffic in accordance with UNISIG Subset 146 Version 4.0.0. **(M)**

The following items of UNISIG Subset 146 version 4.0.0 do not apply:

- 5.4.3.5.
- 5.4.3.6.
- 5.4.3.7.
- 5.4.3.8.

3.2.4 IPSec

3.2.4.1 The VPN component shall protect network traffic in accordance with BSI TR-02102-3 [3] (Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)). **(M)**

3.2.5 WireGuard

3.2.5.1 An alternative to the protocols mentioned before is the WireGuard protocol [2]. **(I)**

3.3 Comparison of Protocols

3.3.1.1 TLS-based VPNs and IPSec are widely used and have been implemented in the railway domain already. **(I)**

3.3.1.2 WireGuard is a new protocol and is not published by recognized standards organisation. **(I)**

[2] More information on WireGuard is available here: https://www.wireguard.com/

3.3.1.3 TLS-based VPNs are only one category of VPN protocols, which may result in different levels of security between different TLS-based VPN protocols. **(I)**

3.4 Comparison of Authentication Methods

3.4.1 Protection of Network Traffic via Untrusted Networks

3.4.1.1 If a PKI is available and accessible by the VPN components, the VPN component shall use certificates for authentication. **(M)**

3.4.1.2 If a PKI is available and cannot be reached by the VPN components, the VPN component shall use certificates for authentication. **(M)**

3.4.1.3 If a PKI is available and cannot be reached by the VPN components, the PKI shall issue certificates to the VPN component without reference to a CRL endpoint. **(M)**

3.4.1.4 If a PKI is not available, the VPN component shall use Pre-Shared Keys[3] for authentication. **(M)**

3.4.2 Protection of Remote Connections

3.4.2.1 The VPN component shall use certificates for authentication. **(M)**

4 Physical protection

4.1.1.1 The railway shall provide physical protection for the VPN component. **(M)**

4.1.1.2 The railway shall ensure the physical protection of the cryptographically unprotected part of the link. **(M)**

5 Homologation

5.1 Safety

5.1.1.1 The railway shall prove that the VPN component does not adversely affect the safety communication layer. **(M)**

5.1.1.2 This can be achieved, for example, by proving that the VPN component does not have the capability to interpret the safety communication layer. **(I)**

5.2 Security

5.2.1.1 The railway shall prove that the VPN component does not adversely affect the security of the system. **(M)**

5.2.1.2 The railway shall use VPN components that are certified to recognized security standards. **(M)**

5.2.1.3 An accepted security standard is e.g. Common Criteria. **(I)**

5.2.1.4 The railway shall prove that at least the same level of protection is maintained according to the network categories of EN 50159:2010 [4]**. (M)**

5.2.1.5 The railway shall prove that at least the same level of protection is achieved in accordance with requirements of IEC 62443-3-3 [5]. **(M)**

[3] Details on recommendations for Pre-Shared Keys are available in NIST SP 800-57 Part 2

5.3 Reliability, Availability, Maintainability (RAM)

5.3.1.1 If the VPN connection is used to transfer safety traffic, the railway shall prove that the required QoS parameters are achieved. **(M)**

5.3.1.2 The railway shall prove that the RAM requirements are met. **(M)**

6 Network Audit (Logging)

6.1.1.1 The VPN component shall provide log data to the SIEM in accordance with the EU-Rail Shared Cybersecurity Services Specification [7]. **(M)**

7 Lifecycle Management

7.1.1.1 The railway shall check the applicability of the requirements of the EU-Rail Security Program Requirements Specification [8]. **(M)**