VÖV UTP

Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100

Nachweisführung Datennetze

Safety und Security

RTE – Regelwerk Technik Eisenbahn

D

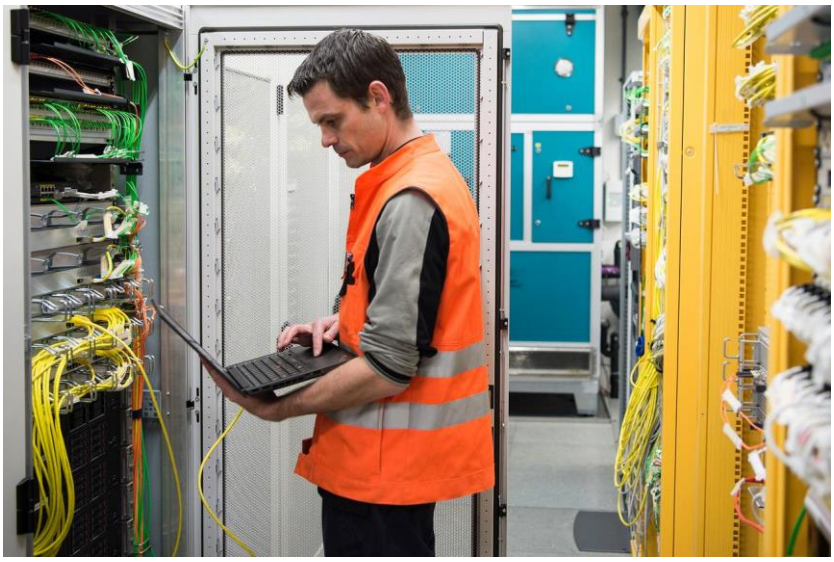
RTE 28100

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Herausgeber VöV **Erarbeitet durch** Projektgruppe VöV	**Ausgabedatum** 09.04.2024 **Freigabe** PL RTE	**Zuordnung** – **Ersatz für** –
Verteiler Bahnunternehmen des VöV Bundesamt für Verkehr BAV RTE-Webshop/RTE-Download (rte.voev.ch)	**Inkrafttreten** Das Inkrafttreten dieser Regelung legt jedes Eisenbahnunternehmen für sich selbst fest.	**Sprachfassungen** d, f **Anzahl Seiten** 162

Nachweisführung Datennetze

Safety und Security



© VöV

Anwendungsbedingungen für das Regelwerk Technik der schweizerischen Eisenbahnen (RTE)

Bei der Anwendung der Dokumente ist zu beachten, dass sie ausschliesslich für die Bedürfnisse der Schweizer Eisenbahnen und Unternehmen im Bereich öV verfasst und für diesen Gebrauch bestimmt sind. Eine korrekte Anwendung setzt somit eine entsprechende Ausbildung und Praxis voraus. Das Regelwerk RTE beschränkt sich auf zwei Arten von Dokumenten:

- Die R-Regelungen sind Ergänzungen bzw. Lösungsvorschläge zu hoheitlichen Erlassen und Normen mit Regelungs- bzw. Weisungscharakter.
- Die D-Regelungen umfassen Handbücher und Dokumentationen als Empfehlungen und Hilfsmittel zur Arbeitsunterstützung oder bilden in Ausnahmefällen den Stand der Technik und die gelebte Praxis im Hinblick auf eine Standardisierung ab.

Die im Dokument in männlicher Form enthaltenen Formulierungen gelten gleichermassen für weibliche oder diverse Personen.

Der Verband öffentlicher Verkehr (VöV) sowie die an der Erstellung dieser Regelung des Regelwerks Technik Eisenbahn (RTE) beteiligten Personen haften nicht für Schäden, die durch die Verwendung von Informationen aus dieser Regelung entstehen können. Alle Angaben erfolgen ohne Gewähr für die Vollständigkeit oder Richtigkeit.

Projektgruppe VöV

Leitung

Werner Kurfess, Schweizerische Bundesbahnen (SBB), Personenverkehr, Bern (bis 12.2022)
Kurt Maier, Schweizerische Bundesbahnen (SBB), Infrastruktur Telecom, Bern (ab 01.2023)

Mitglieder

Patrick Favre, Bundesamt für Verkehr (BAV), Bern
Martin Gerber, Regionalverkehr Bern-Solothurn (RBS), Worblaufen
Stefan Hofmann, Schweizerische Südostbahn (SOB), Herisau
Jan Hohenauer, Schweizerische Bundesbahnen (SBB), Bern
Emmerich Horvath, Zentralbahn (ZB), Stansstad
Tobias Hubschmid, Bundesamt für Verkehr (BAV), Bern
Andreas Klopfenstein, BLS AG, Bern
Alfons Noti, Matterhorn Gotthard Bahn (MGB), Brig
Christoph Preisig, Appenzeller Bahnen (AB), Herisau
Markus Roth, Rhätische Bahn (RhB), Landquart

Projektunterstützung

Kurt Maier, Schweizerische Bundesbahnen (SBB), Infrastruktur Telecom, Bern

Lektorat

Werner Kurfess, IROWE Consulting, Naters (ab Juni 2023)
Urs Walser, Verband öffentlicher Verkehr (VöV), Bern

Nutzungsrecht Abbildungen

Mit © Electrosuisse/CENELEC: Gemäss Bestätigung Electrosuisse vom 10.06.2024

Herausgeber

VöV Verband öffentlicher Verkehr
System Bahn
Dählhölzliweg 12, CH-3005 Bern
www.voev.ch, RTE@voev.ch

RTE-Webshop

rte.voev.ch

ISBN 978-3-907469-18-7

© Verband öffentlicher Verkehr, Bern, April 2024

Änderungsgeschichte

Datum	Änderungen
09.04.2024	1. Ausgabe

© VöV

Vorwort

Datennetze spielen eine wichtige Rolle für einen sicheren Bahnbetrieb. Sie sind zum Beispiel Bestandteil von Sicherungsanlagen und Leittechniksystemen und dienen unter anderem dem Informationsaustausch zwischen sicherheitsrelevanten Anwendungen.

Die vorliegende RTE-Regelung zeigt auf, was beim Einsatz von Infrastruktur-Datennetzen bei Bahnunternehmen zu beachten ist, insbesondere was Safety und Security betrifft.

Die Betreiberin eines Datennetzes muss während des gesamten Lebenszyklus sicherstellen, dass notwendige Anforderungen erfüllt werden. Dazu gehören die folgenden Aspekte:

- Konformität mit hoheitlichen Vorgaben (Gesetzen, Verordnungen, Richtlinien)
- Safety-Anforderungen (Anwendungsbedingungen, z.B. bezüglich der Netzkategorie gemäss SN EN 50159)
- Security-Anforderungen (Handbuch Cybersecurity für den öffentlichen Verkehr, Information Security Management System gemäss AB-EBV, etc.)
- Zuverlässigkeit, Verfügbarkeit und Wartbarkeit (RAM)
- Technische Parameter wie Bandbreite oder Verzögerung (Anwendungsbedingungen)

Da der Fokus dieser RTE-Regelung bei Safety und Security liegt, soll sie vor allem zu den folgenden Fragen angemessene und zweckmässige Antworten geben:

- Wie stellt man sicher, dass keine nicht akzeptablen Safety- und Security-Risiken bei der Aufschaltung und dem Betrieb von sicherheitsrelevanten Anwendungen auf Datennetze entstehen?
- Was ist bei der Projektierung und dem Betrieb von Datennetzen zu beachten, damit sie mit hoheitlichen Regelungen konform sind?
- Wie wird die Zulassung bei Datennetzen gehandhabt, auf denen sicherheits- und betriebsrelevante Anwendungen betrieben werden?

Die vorliegende RTE-Regelung will diejenigen Personen unterstützen, die sich bei der Projektierung und dem Betrieb von Infrastruktur-Datennetzen bei Bahnunternehmen mit solchen Fragen auseinandersetzen.

Da diese RTE-Regelung ziemlich umfangreich ist und verschiedene Fachgebiete behandelt, ist es wichtig sich vor der vertieften Lektüre einen Überblick zu verschaffen und zu entscheiden, welche Teile von besonderer Bedeutung für eine bestimmte Person oder eine ISB sind. Dazu möchten wir speziell auf den Abschnitt 1.3 «Struktur der Regelung» hinweisen. Der Kern dieser RTE-Regelung besteht aus den Kapiteln 5, 6 und 7. Diese drei Kapitel sind als «normativ» gekennzeichnet, um sie von den anderen Kapiteln (und den Anhängen) abzuheben, die einen informativen Charakter haben und das Verständnis der unterschiedlichen Fachgebiete und Standpunkte fördern sollen.

Bern, April 2024

© VöV

1 Allgemeines 11
1.1 Ziele der Regelung 11
1.2 Anwendung 11
1.2.1 Gültigkeitsbereich 11
1.2.2 Abgrenzungen 12
1.3 Struktur der Regelung 12

2 Grundlagen 14
2.1 Hoheitliche Regelungen 14
2.2 Normen 14
2.3 RTE-Regelungen und Regelungen der Bahnen 15
2.4 Richtlinien und Merkblätter 16
2.5 Weitere, eingeschränkt verwendete Grundlagen 16

3 Abkürzungen und Begriffe 17
3.1 Abkürzungen 17
3.2 Begriffe 20

4 Grundsätze 27
4.1 Zulassung von Datennetzen 27
4.1.1 Zulassung bisher 27
4.1.2 Zulassung mit dieser RTE-Regelung 27
4.2 Herausforderungen beim Einsatz von Datennetzen 28
4.3 Datennetze bei Bahnunternehmen 28
4.3.1 Anwendungen im Bahnumfeld 28
4.3.2 Datennetze bei ISB 30
4.3.3 Einteilung von Datennetzen nach Einsatzzweck 30
4.3.4 Einteilung von Datennetzen nach Netzwerk-Kategorien 31
4.4 IT und OT 32
4.5 Safety und Security 34
4.5.1 Unterschiede und Gemeinsamkeiten 34
4.5.2 Risiken 34
4.5.3 Normen zu Safety 35
4.5.4 Normen und Vorgaben zur Security 35

5 Anforderungen an Datennetze (normativ) 37
5.1 Projektanforderungen zu Safety 38
5.2 Projektanforderungen zu Security 38
5.3 Information Security Management System (ISMS) 38
5.4 Anforderungen an die Architektur und Zonierung 39
5.5 Redundanzen und Verfügbarkeit 40
5.6 Anforderungen an Security-Risikoanalysen 40
5.7 Minimaler Target Security Level nach CLC/TS 50701 41
5.8 Anforderungen an die System-Administration und -Konfiguration 41
5.9 Anforderungen an das Betriebskonzept des Datennetzes 44
5.10 Anforderungen an die Dokumentation 45
5.11 Anforderungen an Sachverständige 46
5.12 Anforderungen an die Gebäudesicherheit 46

 © VöV

6 Typenzulassung für Datennetze (normativ) 47

6.1 Typenzulassungsverfahren 47
6.2 Typenzulassung für neue Infrastruktur-Datennetze 47
6.3 Vorgehen bei einer Typenzulassung für Infrastruktur-Datennetze 48
6.3.1 Notwendigkeit eines Typenzulassungsverfahren 48
6.3.2 Typenzulassungsverfahren 50
6.4 Information ans BAV ohne Verfahren 52
6.5 Jährliche Updates ans BAV 53
6.5.1 Updates nach einem Typenzulassungsverfahren 53
6.5.2 Updates nach einer Information zum Datennetzprojekt 54
6.6 Nachträgliche Aufschaltung weiterer Anwendungen 54
6.6.1 Datennetz ohne Typenzulassung 54
6.6.2 Datennetz mit Typenzulassung 54

7 Freigabeprozess für Datennetze (normativ) 55

7.1 Idee und Konzept 55
7.2 Ablauf Freigabeprozess 57
7.2.1 Migration einer bestehenden hoch sicherheitsrelevanten Anwendung 57
7.2.2 Aufschaltung einer neuen hoch sicherheitsrelevanten Anwendung 58
7.2.3 Neuer Release einer bestehenden hohen sicherheitsrelevanten Anwendung 58
7.2.4 Anpassung oder Änderung am Datennetz 58
7.3 Konformitätscheckliste 59
7.4 Risikobeurteilung 60
7.5 Safetyplan 60
7.6 Sachverständigenprüfbericht 60

8 Datennetzprojekte (informativ) 61

8.1 Projektmethodik «klassisch» 61
8.2 Berücksichtigung der RAMS-Phasen gemäss SN EN 50126-1 63
8.3 Agile Vorgehensmodelle 64
8.4 Mitwirkende und ihre Rollen 64

9 Bahnanwendungen (informativ) 65

9.1 Sicherungsanlagen und Telematikanwendungen 65
9.2 Sicherheitsbezogene Anwendungsbedingungen 65
9.3 Beispiele von Bahnanwendungen 66
9.3.1 Disposition, Traffic Management System (TMS) 66
9.3.2 Bahnleittechnik 67
9.3.3 Fernübertragung 67
9.3.4 Stellwerke 67
9.3.5 Aussenanlagen 68
9.3.6 Zugbeeinflussung, Führerstandsignalisierung 68
9.3.7 Zugkommunikation 68
9.3.8 Diagnose 68
9.3.9 Fernwartung 69
9.3.10 Energieversorgung 69

 © VöV

10 Literatur 70
10.1 Hoheitliche Regelungen 70
10.2 Richtlinien, Merkblätter, Studien 70

Anhang A1 – A5 (Allgemein) 72

A1 Hoheitliche Vorgaben 72
A1.1 Schweizerische Gesetzgebung 72
A1.1.1 Eisenbahngesetz (EBG SR 742.101) 72
A1.1.2 Eisenbahnverordnung (EBV SR 742.141.1) 72
A1.1.3 Ausführungsbestimmungen zur Eisenbahnverordnung (AB-EBV) 73
A1.2 Richtlinie Typenzulassung (RL TZL) 75
A1.2.1 Richtlinie Typenzulassung für Elemente von Eisenbahnanlagen (RL TZL) 75
A1.2.2 Vereinfachungen gegenüber der RL TZL 76

A2 Normen zu Safety und Security 77
A2.1 SN EN 50126-1 77
A2.2 SN EN 50126-2 78
A2.3 SN EN 50129 79
A2.4 SN EN ISO/IEC 27000 80
A2.5 SN EN IEC 62443 80
A2.5.1 Normenreihe SN EN IEC 62443 81
A2.5.2 Security Levels 83
A2.5.3 Grundanforderungen 83
A2.5.4 Anforderungen für bestimmte Security Levels 84
A2.5.5 Zonen und Conduits (SN EN IEC 62443-3-2) 85

A3 CLC/TS 50701 86
A3.1 Übersicht 86
A3.2 Kapitel der CLC/TS 50701 86
A3.2.1 Scope (Chap. 1) 87
A3.2.2 Railway system overview (Chap. 4) 87
A3.2.3 Cybersecurity within a railway application lifecycle (Chap. 5) 88
A3.2.4 System definition and initial risk assessment (Chap. 6) 89
A3.2.5 Detailed risk assessment (Chap. 7) 91
A3.2.6 Cybersecurity requirements (Chap. 8) 93
A3.2.7 Cybersecurity assurance and system acceptance for operation (Chap. 9) 93
A3.2.8 Operational, maintenance and disposal requirements (Chap. 10) 93
A3.3 Anhänge der CLC/TS 50701 94
A3.3.1 Annex A (informative) Handling conduits 94
A3.3.2 Annex B (informative) Handling legacy systems 94
A3.3.3 Annex C (informative) Cybersecurity design principles 96
A3.3.4 Annex D (informative) Safety and security 98
A3.3.5 Annex E (informative) Risk acceptance methods 99
A3.3.6 Annex F (informative) Railway architecture and zoning 99
A3.3.7 Annex G (informative) Cybersecurity deliverables content 99
A3.4 Anforderungen pro Security Level 100

A4 SN EN 50159 103
A4.1 Die drei Netzwerk-Kategorien 103
A4.2 Bedrohungen und Schutzmassnahmen 105
A4.3 Bestimmung von Netzwerk-Kategorien 106
A4.3.1 Bestimmung mittels der Vorbedingungen 106
A4.3.2 Bestimmung über die grundsätzlichen Bedrohungen 107
A4.3.3 Bestimmung über die Art der Netzwerktechnologie 108

A5 Gebäudesicherheit für Safety und Security 110
A5.1 Schutzziele Gebäudesicherheit 110
A5.2 Sicherheitsplanung bei Bau- und Umbauprojekten 110
A5.3 Schliesssysteme und Zutrittsregelungen 111
A5.4 Schutzzonen 112

Anhang A6 (SBB-Beispiel) 113

A6 Datennetz Datacom-NG von SBB 113
A6.1 Datacom-NG 113
A6.2 Typenzulassung zu Datacom-NG 113
A6.3 Änderungsprozess 114
A6.3.1 Änderungsprozess zusammen mit anderen KTU 114
A6.3.2 Dokumente des Änderungsprozess mit anderen KTU 114
A6.3.3 Verantwortlichkeiten im Änderungsprozess mit anderen KTU 115

Vorlagen V1 – V7 116

 © VöV