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

D RTE 28100

Démonstration de la sécurité des réseaux de données

Safety et Security

RTE – Ouvrage de référence en matière de technique ferroviaire

D

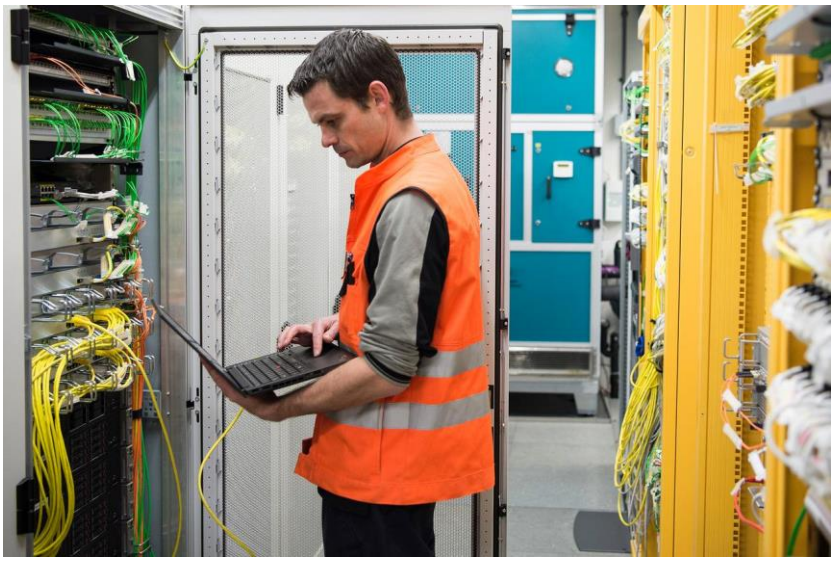
RTE 28100

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

Édité par UTP **Élaboré par** Groupe de projet de l'UTP	**Édité le** 09.04.2024 **Approuvé par** PL RTE	**Subordonné à** – **Remplace** –
Distribution Entreprises ferroviaires de l'UTP Office fédéral des transports (OFT) Webshop RTE/téléchargement RTE (rte.utp.ch)	**Entrée en vigueur** Chaque entreprise de chemin de fer définit la date d'entrée en vigueur de cette réglementation en son sein.	**Versions linguistiques** d, f **Nombre de pages** 162

Démonstration de la sécurité des réseaux de données

Safety et Security



© UTP

Conditions d'utilisation relatives à l'ouvrage de référence en matière de technique ferroviaire (RTE)

Lors de l'utilisation des documents, il convient de garder à l'esprit qu'ils ont été rédigés pour répondre exclusivement aux besoins des chemins de fer et des entreprises de transports publics suisses et qu'ils sont réservés à cet usage. Par conséquent, une utilisation correcte suppose d'avoir suivi une formation tant théorique que pratique dans ce domaine. L'ouvrage de référence RTE se limite à deux niveaux de documents:

- Les documents R viennent compléter ou améliorer les prescriptions souveraines et les normes techniques. Les instructions qu'ils donnent doivent être suivies comme tout règlement.
- Les documents D comprennent des manuels et des documentations servant de recommandations ou d'aides dans le quotidien professionnel ou, à titre exceptionnel, reflètent l'état de la technique et représentent la vraie pratique en vue d'une standardisation.

Les formulations masculines employées dans le présent document valent sans discrimination pour les personnes de tous les sexes.

L'Union des transports publics (UTP) et les personnes ayant participé à l'élaboration de la présente réglementation de l'Ouvrage de référence en matière de technique ferroviaire (RTE) ne sont pas responsables des dommages pouvant résulter de l'utilisation des informations tirées de la réglementation

Groupe de projet de l'UTP

Direction

Werner Kurfess, Chemins de fer fédéraux suisses (CFF), Voyageurs, Berne (jusqu'en décembre 2022)
Kurt Maier, Chemins de fer fédéraux suisses (CFF), Infrastructure Télécom, Berne (depuis janvier 2023)

Membres

Patrick Favre, Office fédéral des transports (OFT), Berne
Martin Gerber, Regionalverkehr Bern-Solothurn (RBS), Worblaufen
Stefan Hofmann, Schweizerische Südostbahn (SOB), Herisau
Jan Hohenauer, Chemins de fer fédéraux suisses (CFF), Berne
Emmerich Horvath, Zentralbahn (ZB), Stansstad
Tobias Hubschmid, Office fédéral des transports (OFT), Berne
Andreas Klopfenstein, BLS SA, Berne
Alfons Noti, Matterhorn Gotthard Bahn (MGB), Brigue
Christoph Preisig, Appenzeller Bahnen (AB), Herisau
Markus Roth, Chemins de fer rhétiques (RhB), Landquart

Assistance de projet

Kurt Maier, Chemins de fer fédéraux suisses (CFF), Infrastructure Télécom, Berne

Traduction

Trad 8, Delémont

Révision

Werner Kurfess, IROWE Consulting, Naters (à partir de juin 2023)
Urs Walser, Union des transports publics (UTP), Berne
Patrick Favre, Office fédéral des transports (OFT), Berne

Droit d'utilisation des illustrations

En indiquant © Electrosuisse/CENELEC: selon la confirmation d'Electrosuisse du 10.06.2024.

Éditeur

Union des transports publics (UTP)
Domaine Système ferroviaire
Dählhölzliweg 12, 3005 Berne
www.utp.ch, RTE@utp.ch

Webshop RTE

rte.utp.ch

ISBN 978-3-907469-19-4

© Union des transports publics, Berne, avril 2024

Historique des modifications

Date	Modifications
09.04.2024	1re édition

© UTP

Avant-propos

Les réseaux de données jouent un rôle important dans la sécurité de l'exploitation ferroviaire. Ils font par exemple partie intégrante des installations de sécurité et des systèmes de commande et servent entre autres à l'échange d'informations entre des applications importantes pour la sécurité.

La présente réglementation RTE indique les éléments à prendre en compte lors de l'utilisation de réseaux de données d'infrastructure par les entreprises ferroviaires, notamment en ce qui concerne la Safety et la Security.

L'exploitant d'un réseau de données doit s'assurer pendant tout le cycle de vie que les exigences requises sont satisfaites. Les aspects suivants en font partie:

- conformité aux prescriptions souveraines (lois, ordonnances, directives);
- exigences de Safety (conditions d'application, p. ex. concernant la classe de réseau selon la norme SN EN 50159);
- exigences de Security (manuel sur la cybersécurité destiné aux entreprises de transports publics, système de management de la sécurité de l'information selon les DE-OCF, etc.);
- fiabilité, disponibilité et maintenabilité (FDM);
- paramètres techniques tels que la bande passante ou le retard (conditions d'application).

Cette réglementation RTE étant essentiellement axée sur la Safety et la Security, elle doit en premier lieu apporter des réponses adéquates et appropriées aux questions suivantes.

- Comment s'assurer qu'aucun risque inacceptable en matière de Safety et de Security ne survienne lors de la mise en ligne et de l'exploitation d'applications importantes pour la sécurité sur les réseaux de données?
- Quels éléments faut-il prendre en compte lors de la planification et de l'exploitation de réseaux de données pour qu'ils soient conformes aux réglementations souveraines?
- Comment l'homologation est-elle gérée pour les réseaux de données sur lesquels sont exploitées des applications importantes pour la sécurité et pour l'exploitation?

La présente réglementation RTE a pour but d'aider les personnes confrontées à de telles questions lors de la planification et de l'exploitation de réseaux de données d'infrastructure dans les entreprises ferroviaires.

Étant donné que cette réglementation RTE est relativement volumineuse et aborde différents domaines spécialisés, il est important d'en avoir une vue d'ensemble avant de la lire en détail et de décider quelles parties sont particulièrement importantes pour une personne ou un gestionnaire d'infrastructure donné(e). Pour ce faire, nous souhaitons attirer tout particulièrement votre attention sur la section 1.3 «Structure de la réglementation». Les chapitres 5, 6 et 7 forment le noyau de cette réglementation RTE. Ces trois chapitres sont identifiés comme «normatifs» afin de les distinguer des autres chapitres (et des annexes), qui ont un caractère informatif et visent à favoriser la compréhension des différents domaines spécialisés et points de vue.

Berne, avril 2024

© UTP

1 Généralités 11
1.1 Buts de la présente réglementation 11
1.2 Utilisation 11
1.2.1 Champ d'application 11
1.2.2 Délimitations 12
1.3 Structure de la réglementation 12

2 Bases 14
2.1 Réglementations souveraines 14
2.2 Normes 14
2.3 Réglementations RTE et réglementations des chemins de fer 15
2.4 Directives et fiches 16
2.5 Autres bases utilisées de manière limitée 16

3 Abréviations et termes 17
3.1 Abréviations 17
3.2 Termes 20

4 Principes 27
4.1 Homologation de réseaux de données 27
4.1.1 Homologation jusqu'à présent 27
4.1.2 Homologation avec cette réglementation RTE 27
4.2 Défis liés à l'utilisation des réseaux de données 28
4.3 Réseaux de données dans les entreprises ferroviaires 28
4.3.1 Applications dans l'environnement ferroviaire 28
4.3.2 Réseaux de données chez les gestionnaires d'infrastructure 30
4.3.3 Classification des réseaux de données en fonction de leur utilisation 30
4.3.4 Classification des réseaux de données par classes de réseaux 31
4.4 TI et TO 32
4.5 Safety et Security 34
4.5.1 Différences et points communs 34
4.5.2 Risques 34
4.5.3 Normes relatives à la Safety 35
4.5.4 Normes et prescriptions relatives à la Security 35

5 Exigences relatives aux réseaux de données (normatif) 37
5.1 Exigences de projet relatives à la Safety 38
5.2 Exigences de projet relatives à la Security 38
5.3 Information Security Management System (ISMS) 38
5.4 Exigences relatives à l'architecture et au zonage 39
5.5 Redondances et disponibilité 40
5.6 Exigences relatives à l'analyse des risques de Security 40
5.7 Target Security Level minimal selon la CLC/TS 50701 41
5.8 Exigences relatives à l'administration et la configuration du système 41
5.9 Exigences relatives au concept d'exploitation du réseau de données 44
5.10 Exigences relatives à la documentation 45
5.11 Exigences relatives aux experts 46
5.12 Exigences relatives à la sécurité des bâtiments 46

 © UTP

6 Homologation de série des réseaux de données (normatif) 47

6.1 Procédure d'homologation de série 47
6.2 Homologation de série de nouveaux réseaux de données d'infrastructure 47
6.3 Procédure d'homologation de série des réseaux de données d'infrastructure 48
6.3.1 Nécessité d'une procédure d'homologation de série 48
6.3.2 Procédure d'homologation de série 50
6.4 Information à l'OFT sans procédure 52
6.5 Transmission de mises à jour annuelles à l'OFT 53
6.5.1 Mises à jour après une procédure d'homologation de série 53
6.5.2 Mises à jour après une information sur le projet de réseau de données 54
6.6 Mise en ligne ultérieure d'autres applications 54
6.6.1 Réseau de données sans homologation de série 54
6.6.2 Réseau de données avec homologation de série 54

7 Processus d'approbation des réseaux de données (normatif) 55

7.1 Idée et concept 55
7.2 Déroulement du processus d'approbation 56
7.2.1 Migration d'une application existante de haute importance pour la sécurité 56
7.2.2 Mise en ligne d'une nouvelle application de haute importance pour la sécurité 57
7.2.3 Nouvelle version d'une application existante de haute importance pour la séc. 57
7.2.4 Adaptation ou modification sur le réseau de données 58
7.3 Check-list de conformité 59
7.4 Évaluation des risques 60
7.5 Plan de sécurité 60
7.6 Rapport d'examen de l'expert 60

8 Projets de réseaux de données (informatif) 61

8.1 Méthodologie de projet «classique» 61
8.2 Prise en compte des phases FDMS selon la norme SN EN 50126-1 63
8.3 Modèles agiles de gestion de projets et de produits 64
8.4 Parties prenantes et leurs rôles 64

9 Applications ferroviaires (informatif) 65

9.1 Installations de sécurité et applications télématiques 65
9.2 Conditions d'application liées à la sécurité 65
9.3 Exemples d'applications ferroviaires 66
9.3.1 Disposition, Traffic Management System (TMS) 66
9.3.2 Technique de commande ferroviaire 67
9.3.3 Télécommande 67
9.3.4 Appareils d'enclenchement 67
9.3.5 Installations extérieures 68
9.3.6 Contrôle de la marche des trains, signalisation en cabine 68
9.3.7 Radio 68
9.3.8 Diagnostic 68
9.3.9 Maintenance à distance 69
9.3.10 Approvisionnement en énergie 69

 © UTP

10 Bibliographie 70
10.1 Règlementations souveraines 70
10.2 Directives, fiches, études 70

Annexes A1-A5 (général) 72

A1 Prescriptions souveraines 72
A1.1 Législation suisse 72
A1.1.1 Loi sur les chemins de fer (LCdF RS 742.101) 72
A1.1.2 Ordonnance sur les chemins de fer (OCF RS 742.141.1) 72
A1.1.3 Dispositions d'exécution de l'ordonnance sur les chemins de fer (DE-OCF) 73
A1.2 Directive Homologation de série (dir. HdS) 75
A1.2.1 Directive Homologation de série pour éléments d'installations ferroviaires 75
A1.2.2 Simplifications par rapport à la dir. HdS 76

A2 Normes relatives à la Safety et la 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 Série de normes SN EN IEC 62443 81
A2.5.2 Security Levels 83
A2.5.3 Exigences de base 83
A2.5.4 Exigences relatives aux Security Levels 84
A2.5.5 Zones et conduits (SN EN IEC 62443-3-2) 85

A3 CLC/TS 50701 86
A3.1 Vue d'ensemble 86
A3.2 Chapitres de la 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 Annexes de la 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 Exigences selon les Security Levels 100

 © UTP

A4 SN EN 50159 103
A4.1 Les trois classes de réseau 103
A4.2 Menaces et mesures de protection 105
A4.3 Détermination des classes de réseau 106
A4.3.1 Détermination basée sur les conditions préalables 106
A4.3.2 Détermination basée sur les menaces fondamentales 107
A4.3.3 Détermination basée sur le type de technologie de réseau 108

A5 Sécurité des bâtiments pour la Safety et la Security 110
A5.1 Objectifs de protection de la sécurité des bâtiments 110
A5.2 Planification de la sécurité dans les projets de construction et de transformation 110
A5.3 Systèmes de fermeture et réglementations d'accès 111
A5.4 Zones de protection 112

Annexe A6 (spécifique aux CFF) 113

A6 Réseau de données Datacom-NG des CFF 113
A6.1 Datacom-NG 113
A6.2 Homologation de série de Datacom-NG 113
A6.3 Processus de modification 114
A6.3.1 Processus de modification en relation avec d'autres ETC 114
A6.3.2 Documents du processus de modification avec d'autres ETC 114
A6.3.3 Responsabilités dans le processus de modification avec d'autres ETC 115

Modèles V1-V7 116

 © UTP