Ministry of Transport of the Slovak Republic
Department of Road Transport and Roads

TS 119

TECHNICAL SPECIFICATIONS

Technical facilities. Common requirements.

effective date: xx. xx. 202x

CONTENTS

1 Introductory chapter

1.1 Mutual recognition

Where these specifications lay down a requirement for conformity with any part of a Slovak standard ('Slovak Technical Standard') or other technical specifications, this requirement may be satisfied by ensuring conformity with:

(a) a standard or code of good practice issued by the national standardisation body or an equivalent body of an EEA State or Turkey;

(b) any international standard acknowledged by any EEA state or Turkey as the best practice standard or codex;

(c) a technical specification recognised by a public authority of an EEA State or Turkey as a standard; or

(d) a European technical assessment issued in accordance with the procedure laid down in Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/EEC, as amended.

The above sub-paragraphs shall not apply if it is demonstrated that the standard in question does not guarantee the appropriate level of functionality and safety.

'EEA State' means a State party to the Agreement on the European Economic Area signed in Oporto on 2 May 1992, as amended.

'Slovak standard' ('Slovak Technical Standard') means any standard issued by the Office of Standards, Metrology and Testing of the Slovak Republic, including transposed European or other international or foreign standards.

1.2 Subject of the Technical Specifications (TS)

These technical specifications (TS) apply to the design, implementation and operation of technical facilities for roads pursuant to legislative requirements, for technical facilities for roads and related equipment and power facilities. They define common requirements.

1.3 Purpose of the TS

The purpose of these TS is to establish common requirements for technical facilities for roads. They contain common requirements for .equipment, power and technical facilities for road structures.

1.4 Scope of application of the TS

The use of these TS is defined for common requirements for equipment, power and technical facilities for road structures. The TS are intended for road designers, contractors, investors, builders and managers.

1.5 Preparation of the TS

These TS were prepared by FIMAU, s.r.o. on the basis of an order from the Slovak Road Administration (SSC). Responsible authors are Associate Professor RNDr. Stanislav Urgela, PhD., phone: +421 949 641 712, email: s.urgela@fimau.com and Ing. Vojtech Tóth, phone: + 421903446429, email: toth@elhyco.sk.

1.6 Distribution of the TS

After approval, the electronic version of the TS will be published on the SSC website: www.ssc.sk (Technické predpisy rezortu [Departmental Technical Regulations]).

1.7 Effective date of the TS

These TS shall take effect on the date on the title page.

1.8 Superseded regulations

These TS partially replace TS 029 Equipment, infrastructure and technical facility systems for roads (Ministry of Post, Transport and Communications of the SR), 2008 as follows:

Replaced part of TS 029	Replacing part of these TS
Chapter 3	Chapter 3

Changes in references between TS 029 and this regulation in TS 030:

Article of TS 030 referring to TS 029	Article/Chapter of these TS specifying the issue in question	Note
3.1.1	TS	**If 'TS' is written in the second column of the table, the reference refers to the entire TS. If '-' is indicated in this third column of the table, this means that no additional note is needed.**
3.1.3	3.1	-
3.4.1	8	Through a reference we can use TS 019 to get to other TPR and standards that are listed in TS 019
3.4.2	8	See also Note to 3.4.1
3.4.5.1	8	See also Note to 3.4.1
3.4.5.2	3.2.1	-
4.8.4.4	3.3	Classes of infrastructure importance are applied
5.5.5	3	Except for real-time classes that are not applied
6.2.5.2	3.1.1, 6.1.2.3	Road technical facility level is a modified term, not identical to the previous Technology Grade Class
6.4.2.3	3.1.1, 4.4.2	See also the two preceding notes 6.2.5.2
6.5.5	3	-
7.2 (2)	3	See also Note to 6.2.5.2
7.6.5	3, 4.5.1	-
8.6.8	3	Except for proxy units, which are not addressed in these TS

Changes to references between TS 029 and this regulation in TS 082:

Article in TS 082 referring to TS 029	Article/Chapter of these TS specifying the issue in question	Note
2 (1)*	2.2.3, 3.3	For the term 'tunnel road section' introduced in TS 082, the term 'technological transport section' shall apply pursuant to these TS.
13.2.1.1	3.3	-
13.2.1.2	3.3	-

*numbering of Articles of Chapter 13, Addendum B

Changes to references between TS 029 and this regulation in TS 093:

Article in TS 093 referring to TS 029	Article/Chapter of these TS specifying the issue in question	Note
3.2.2	3.1	This involves classification in a reliability and availability class
4.2 (1)	3.1	-
4.2 (2)	3.1	Other control units classified in reliability and availability class B
4.2 (3)	3.1	-

Changes to references between TS 029 and this regulation in TS 099:

Article in TS 099 referring to TS 029	Article/Chapter of these TS specifying the issue in question	Note
18.1.1	3.4	-

1.9 Related and cited legislation

[Z1] Act No 135/1961, on roads (the Road Act), as amended;
[Z2] Federal Ministry of Transport Decree No 35/1984 implementing the Road Act;
[Z3] Act No 8/2009 on road traffic and amending certain acts, as amended;
[Z4] Decree of the Ministry of Interior of the Slovak Republic No 9/2009 implementing the Road Act and amending certain acts, as amended;
[Z5] Act No 133/2013 on building materials and amending certain acts, as amended;
[Z6] Slovak Ministry of Transport, Construction and Regional Development Decree No 162/2013, stipulating a list of construction product groups and systems for assessing parameters, as amended;
[Z7] Regulation (EC) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/EEC, as amended
[Z8] Regulation of the Government of the Slovak Republic No 344/2006 on minimum safety requirements for tunnels in the road network;
[Z9] Act No 50/1976 on land-use planning and the building code (the Building Act). (Effective from 1 April 2023 to 31 March 2024);
[Z10] Act No 138/1992 of the Slovak National Council on authorised architects and authorised civil engineers;
[Z11] Act No 145/1995 of the National Council of the Slovak Republic on administrative fees;
[Z12] Act No 56/2012 on road transport;
[Z13] Act No 317/2012 on intelligent transport systems in road transport and amending certain acts;
[Z14] Act No 106/2018 on the operation of vehicles in road traffic and amending certain acts;
[Z15] Act No 185/2015, the Copyright Act;
[Z16] Act No 69/2018 on cybersecurity and amending certain acts;
[Z17] Act No 106/2018 on the operation of vehicles in road traffic and amending certain acts;
[Z18] Decree No 134/2018 of the Ministry of Transport and Construction of the SR establishing details of the operation of vehicles in road traffic;
[Z19] Decree No 362/2018 of the NSA establishing content of security measures, content and structure of security documentation and scope of general security measures;
[Z20] Act No 95/2019 on information technology in public administration and amending certain acts;
[Z21] Decree No 30/2020 of the Ministry of the Interior of the Slovak Republic on traffic signage;
[Z22] Act No 200/2022 on spatial planning. (Effective 01.04.2024);
[Z23] Act No 201/2022 on construction. (Effective 01.04.2024);
[Z24] Act No 265/2022 on publishers of publications and on the media and audiovisual register and amending certain acts (the Publications Act);
[Z25] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport;
[Z26] Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council as regards harmonised provision of interoperable EU-wide eCall;
[Z27] Commission Delegated Regulation (EU) No 885/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council on Intelligent Transport Systems with regard to provision of information services for safe and secure parking places for trucks and commercial vehicles;
[Z28] Commission Delegated Regulation (EU) No 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures

for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users;

[Z29] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services;

[Z30] Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services;

[Z31] Commission Delegated Regulation (EU) 2022/670 of 2 February 2022 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services;

[Z32] Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC;

[Z33] Council recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure;

[Z34] Draft EU Cyber Defence Policy – Opinion of the Consultative Commission on Industrial Change (CCMI). Joint Communication to the European Parliament and the Council. EU cyber defence policy [JOIN(2022) 49 final] of 31 March 2023;

[Z35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

[Z36] Act No 18/2018 on personal data protection and amending certain acts;

[Z37] Commission Implementing Decision (EU) 2017/863 of 18 May 2017 updating the European Union Public Open Source Software Licence (EUPL) to further promote the sharing and reuse of software developed by public administrations;

[Z38] Decree No 179/2020 of the Office of the Deputy Prime Minister of the Slovak Republic for Investment and Informatisation, establishing the method of categorisation and content of security measures of public administration information technologies;

[Z39] Commission Delegated Regulation (EU) 2022/1012 of 7 April 2022 supplementing Regulation (EC) No 561/2006 of the European Parliament and of the Council as regards the establishment of standards specifying the level of service and security of safe and secure parking areas and their certification procedures;

[Z40] Act No 429/2022 amending certain acts relating to the development of automated vehicles;

[Z41] Act No 473/2005 on the provision of services in the field of private security and amending certain acts (the Private Security Act);

[Z42] Decree No 634/2005 of the Ministry of the Interior of the Slovak Republic implementing certain provisions of Act No 473/2005 on the provision of services in the field of private security and amending certain acts (the Private Security Act);

[Z43] Act No 452/2021 on electronic communications;

[Z44] Vienna, 8 November 1968, Notification of the Ministry of Foreign Affairs of the Slovak Republic No 53/1994;

[Z45] Decree of the Ministry of the Interior of the Slovak Republic No 94/2004 laying down technical requirements for fire safety in the construction and use of buildings, as amended

[Z46] Regulation of the Government of the Slovak Republic No 127/2016 on electromagnetic compatibility (as amended by Slovak Government Regulation No 331/2019, as amended

[Z47] Act No 124/2006 on occupational health and safety and amending certain acts

[Z48] Decree No 251/2011 of the Ministry of Transport, Construction and Regional Development of the Slovak Republic laying down the details of road safety management, as amended by No 254/2022

1.10 Related and cited standards

STN 01 3420	Construction drawings. Common requirements and drawing
STN 33 2000-1	Low-voltage electrical installations. Part 1: Fundamental principles, assessment of general characteristics, definitions
STN 33 2000-2	International Electrotechnical Vocabulary. Chapter 826: Electrical wiring in buildings.
STN 33 2000-4-41	Low-voltage electrical installations. Part 4-41: Safety assurance. Protection against electrical shock

STN 33 2000-4-42	Low-voltage electrical installations. Part 4-42: Safety assurance. Protection against the effects of heat
STN 33 2000-5-51	Electrical wiring in buildings. Part 5-51: Selection and erection of electrical equipment. Common rules
STN 33 2000-5-52	Low-voltage electrical installations. Part 5-52: Selection and erection of electrical installation. Electrical wiring
STN 33 2000-5-53	Low-voltage electrical installations. Part 5-53: Selection and erection of electrical equipment. Switching and control equipment
STN 33 2000-5-54	Low-voltage electrical installations. Part 5-54: Selection and erection of electrical equipment. Earthing arrangements and protective conductors
STN 33 2000-5-551	Low-voltage electrical installations. Part 5-55: Selection and erection of electrical equipment. Other facilities. Section 551: Low-voltage generators
STN 33 2000-5-559	Low-voltage electrical installations. Part 5-559: Selection and erection of electrical equipment. Luminaires and lighting installations
STN 33 2000-6	Low-voltage electrical installations. Part 6: Inspection
STN 33 2000-7-712	Low-voltage electrical installations. Part 7-712: Requirements for special installations or locations. Photovoltaic (PV) systems
STN 33 3320	Electrical connections
STN 34 1050	STN electrical regulations. Regulations for laying power lines
STN 34 1610	STN electrical regulations. Power distribution in industrial plants
STN 34 3100	Safety requirements for operation and work on electrical installations
STN 73 6100	Terminology of roads
STN 73 6101	Design of roads and motorways
STN 73 7507	Design of road tunnels
STN 73 6201	Standard Specifications for Bridges
STN 73 6056	Parking areas for road vehicles
STN 73 6005:	Space arrangement of conduits of technical equipment
STN 92 0203	Fire safety of buildings. Continuous power supply during fire
STN EN 1317-1 (73 6030)	Road restraint systems. Part 1: Terminology and general criteria for test methods
STN EN 1990 (73 0031)	Eurocode. Basis of structural design
STN EN 1991-1-1 (73 0035)	Eurocode 1. Actions on structures. Part 1-1: General actions. Volumetric masses, own weights and utility loads of buildings
STN EN 1991-1-2 (73 0035)	Eurocode 1. Actions on structures. Part 1-2: General loads. Loading of structures stressed by fire
STN EN 1991-1-3 (73 0035)	Eurocode 1. Actions on structures. Part 1-3: General actions. Snow loads
STN EN 1991-1-4 (73 0035)	Eurocode 1. Actions on structures. Part 1-4: General actions. Wind loads
STN EN 1991-1-5 (73 0035)	Eurocode 1. Actions on Structures. Part 1-5: General actions. Thermal actions
STN EN 1991-1-6 (73 0035)	Eurocode 1: Actions on structures. Part 1-6: General actions. Actions during construction
STN EN 1991-1-7 (73 0035)	Eurocode 1. Actions on structures. Part 1-7: General actions. Accidental
STN EN 1991-2 (73 0035)	Eurocode 1. Actions on structures. Part 2: Traffic loads on bridges
STN EN 1992 (73 1201)	Eurocode 2. Design of concrete structures
STN EN 1993 (73 1401)	Eurocode 3. Design of steel structures
STN EN 1994 (73 2089)	Eurocode 4. Design of composite steel and concrete structures
STN EN 1996 (73 0851)	Eurocode 6. Design of masonry structures
STN EN 1997 (73 0091)	Eurocode 7. Geotechnical design

STN EN 1998 (73 0036)	Eurocode 8. Design of structures for earthquake resistance
STN EN 1999 (73 1501)	Eurocode 9. Design of aluminium structures
STN EN 12368 (73 6022)	Traffic control equipment. Signal heads
STN EN 12966+A1 (73 7040)	Vertical traffic signs. Traffic signs with variable symbols
STN EN 13321-1 (74 7302)	Open data communication in building automation, controls and building management. Home and building electronic systems Part 1: Product and system requirements
STN EN 14908-5 (74 7306)	Open data communication in building automation, controls and building management. Network protocol. Part 5: Implementation guide
STN EN 15518-1 (30 3361)	Winter maintenance equipment. Road meteorology information systems. Part 1: Overall definitions and parts
STN EN 15518-2 (30 3361)	Winter maintenance equipment. Road meteorology information systems. Part 2: Road meteorology – recommended observation and forecast
STN EN 15518-3 (30 3361)	Winter maintenance equipment. Road meteorology information systems. Part 3: Requirements for measured values of stationary installations
STN P CEN/TS 15518-4 (30 3361)	Winter maintenance equipment. Road meteorology information systems. Part 4: Test methods for stationary installations
STN EN 16062 (01 8590)	Intelligent Transport Systems. Electronic security. ECall High Level Application Protocols (HLAPs) using GSM/UMTS circuit switched networks
STN EN 16072 (01 8591)	Intelligent Transport Systems. Electronic security. Operational requirements for pan-European eCall
STN EN 16157-1 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information. Part 1: Background and framework
STN EN 16157-2 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information. Part 2: Location reference
STN EN 16157-3 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information. Part 3: Situation publication
STN EN 16157-4 (01 8594)	Intelligent Transport Systems. DATEX II data exchange specifications for traffic management and information. Part 4: VMS publication
STN EN 16157-5 (01 8594)	Intelligent Transport Systems. DATEX II data exchange specifications for traffic management and information. Part 5: Display of measured and processed data
STN P CEN/TS 16157-6 (01 8594)	Intelligent Transport Systems. Data exchange specifications in Datex II for traffic management and traffic information. Part 6: Display of parking
STN EN 16157-7 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information. Part 7: Common data elements
STN P CEN/TS 16157-8 (01 8594)	Intelligent Transport Systems. Data exchange specifications in Datex II for traffic management and traffic information. Part 8: Publication of traffic management and extensions for the urban environment
STN P CEN/TS 16157-9 (01 8594)	Intelligent Transport Systems. DATEX II data exchange specifications for traffic management and information. Part 9: Display control of traffic signals intended for the urban environment
STN P CEN/TS 16157-10 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information. Part 10: Publication of power infrastructure
STN P CEN/TS 16157-11 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information.

	Part 11: Publication of machine-interpretable traffic control
STN P CEN/TS 16157-12 (01 8594)	Intelligent Transport Systems. Data exchange specifications in DATEX II for traffic management and traffic information. Part 12: Publication related to structures
STN EN 16803-1 (31 0545)	Space. GNSS-based positioning application for Intelligent Transport Systems (ITS) in road transport. Part 1: System engineering definitions and procedures to determine and assess performance
STN EN 16803-2 (31 0545)	Space. GNSS-based positioning application for Intelligent Transport Systems (ITS) in road transport. Part 2: Assessment of the baseline performance of GNSS-based positioning terminals
STN EN 17609 (74 7402)	Automation in buildings and control systems. Control applications
STN EN 17632-1 (73 9019)	Building Information Modelling (BIM). Semantic modelling and linking (SML). Part 1: General modelling patterns
STN EN 302 571 V2.1.1	Intelligent Transport Systems (ITS) Radio communication equipment operating in the 5855 MHz to 5925 MHz frequency band. Harmonised EN covering essential requirements pursuant to Article 3.2 of Directive 2014/53/EU
STN EN 50160 (33 0121)	Characteristics of the voltage of electricity supplied from the public electricity grid
STN EN 50171 (36 0630)	Central security power supply systems
STN EN 50293	Road traffic signal systems Electromagnetic compatibility
STN EN 50468	Resistibility requirements to overvoltages and overcurrents due to lightning for equipment having telecommunication ports
STN EN 50556 (36 5601)	Road traffic signal systems
STN EN 60529 (33 0330)	Degrees of protection provided by enclosures (IP Code)
STN EN 61069-1 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 1: Terminology and basic concepts
STN EN 61069-2 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 2: Assessment methodology
STN EN 61069-3 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 3: System functionality assessment
STN EN 61069-4 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 4: Assessment of system performance
STN EN 61069-5 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 5: Assessment of system reliability
STN EN 61069-6 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 6: Assessment of system operability
STN EN 61069-7 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 7: Assessment of system safety
STN EN 61069-8 (18 0451)	Industrial process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 8: Assessment of undefined system properties
STN EN 61131-1 (18 7050)	Programmable controllers. Part 1: General information
STN EN 61131-3 (18 7050)	Programmable controllers. Part 3: Programming languages
STN EN 61131-5 (18 7050)	Programmable controllers. Part 5: Communication
STN EN IEC 61131-9 (18 7050)	Programmable logic controllers. Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI).

STN EN IEC 61131-10 (18 7050)	Part 10: XML formats for data exchange between programs according to IEC 61131-3
STN EN 61158-2 (18 4020)	Industrial communication networks. Specifications of operational buses. Part 2: Physical layer specification and service definition
STN EN 61175-1 (01 3381)	Industrial systems, installations and equipment and industrial products. Designation of signals. Part 1: Basic rules
STN EN 61439 (35 7107)	Low-voltage switchgear
STN EN IEC 61439-1 (35 7107)	Low-voltage switchgear. Part 1: General rules
STN EN 61508-1 (18 4020)	Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements
STN EN 61508-2 (18 4020)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Functional safety of electrical/electronic/programmable electronic safety-related systems
STN EN 61508-3 (18 4020)	Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements
STN EN 61508-4 (18 4020)	Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions and abbreviations
STN EN 61557 (35 6230)	Electrical safety in low voltage distribution systems up to 1000 VAC and 1500 VDC.
STN EN 61558 (35 1330)	Safety of transformers, chokes, power supplies and their combinations.
STN EN 61850-3 (33 4850)	Communication networks and electrical station automation systems. Part 3: General requirements
STN EN 61850-4 (33 4850)	Communication networks and electrical station automation systems. Part 4: System and project management
STN EN 61850-5 (33 4850)	Communication networks and electrical station automation systems. Part 5: Communication requirements for instrument function and models
STN EN 61850-6 (33 4850)	Communication networks and electrical station automation systems. Part 6: Language to describe configuration for communication in stations with intelligent electronic devices (IED)
STN EN 61850-7-1 (33 4850)	Communication networks and electrical station automation systems. Part 7-1: Basic communication structure. Principles and models
STN EN 62264-1 (18 4411)	Enterprise-control system integration. Part 1: Models and terminology
STN EN 62264-2 (18 4411)	Enterprise-control system integration. Part 2: Objects and attributes for the integration of enterprise control systems
STN EN 62264-3 (18 4411)	Enterprise-control system integration. Part 3: Production plant management activity models
STN EN 62264-4 (18 4411)	Enterprise-control system integration. Part 4: Attributes of the object model for integration of the management of production sites
STN EN 62264-5 (18 4411)	Enterprise-control system integration. Part 5: Business to manufacturing transactions
STN EN 62264-6 (18 4411)	Enterprise-control system integration. Part 6: Messaging service model
STN EN 62271-200 (35 4220)	High-voltage switchgear and controlgear. Part 200: AC metal-enclosed switchgear and controlgear for rated voltages above 1 kV and up to and including 52 kV
STN EN 62271-201 (35 4220)	High-voltage switchgear and controlgear. Part 201: AC solid-insulation enclosed switchgear and controlgear for rated voltages above 1 kV and up to and including 52 kV
STN EN 62271-202 (35 4220)	High-voltage switchgear and controlgear. Part 202: High

	voltage/low voltage prefabricated substations
STN EN 62305-1 (34 1390)	Protection against lightning. Part 1: General principles
STN EN 62305-3 (34 1390)	Protection against lightning. Part 3: Physical damage to structures and life hazard
STN EN 62439-1 (18 4020)	Industrial communication networks. High availability automation networks. Part 1: General concepts and calculation methods
STN EN 62439-2 (18 4020)	Industrial communication networks. High availability automation networks. Part 2: MRP protocol (Media Redundancy Protocol)
STN EN IEC 62439-3 (18 4020)	Industrial communication networks. High availability automation networks. Part 3: PRP Protocol (Parallel Redundancy Protocol) and High Standby Circular Network (HSR)
STN EN 62439-4 (18 4020)	Industrial communication networks. High availability automation networks. Part 4: CRP Protocol (Cross-network Redundancy Protocol)
STN EN 62439-5 (18 4020)	Industrial communication networks. High availability automation networks. Part 5: BRP protocol (Beacon Redundancy Protocol)
STN EN 62439-6 (18 4020)	Industrial communication networks. High availability automation networks. Part 6: DRP Protocol (Distributed Redundancy Protocol)
STN EN 62439-7 (18 4020)	Industrial communication networks. High availability automation networks. Part 7: RRP Protocol (Ring-based Redundancy Protocol)
STN EN 62657-1 (18 4020)	Industrial communication networks. Radio communications networks. Part 1: Radio communication requirements and spectrum considerations
STN EN 62657-2 (18 4020)	Industrial communication networks. Radio communications networks. Part 2: Coexistence management
STN EN IEC 62657-3 (18 4020)	Industrial communication networks. Coexistence of wireless systems. Part 3: Formal description of automated coexistence management and application guidance
STN EN IEC 62657-4 (18 4020)	Industrial communication networks. Coexistence of wireless systems. Part 4: Coexistence management with central coordination of wireless applications
STN EN IEC 62443-3-2 (36 9060)	Security for industrial automation and control systems. Part 3-2: Security risk assessment for system design
STN EN IEC 62443-3-3 (36 9060)	Industrial communication networks. Network and system security. Part 3-3: System security requirements and security level
STN EN IEC 62443-4-1 (36 9060)	Security for industrial automated control systems. Part 4-1: Secure product development lifecycle requirements
STN EN IEC 62443-4-2 (36 9060)	Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components
STN EN IEC 62832-1 (18 0460)	Industrial process measurement, control and automation. Digital factory framework. Part 1: General principles
STN EN IEC 62832-2 (18 0460)	Industrial process measurement, control and automation. Digital factory framework. Part 2: Model elements
STN EN IEC 62832-3 (18 0460)	Industrial process measurement, control and automation. Digital factory framework. Part 3: Application of Digital Factory for life cycle management of production systems
STN IEC 60050-161 (33 0050)	International Electrotechnical Vocabulary. Chapter 161: Electromagnetic compatibility
STN IEC 60050-351 (33 0050)	International Electrotechnical Vocabulary. Part 351: Control technology
STN IEC 60050-371 (33 0050)	International Electrotechnical Vocabulary. Chapter 371: Telecontrol
STN IEC 60050-701 (33 0050)	International Electrotechnical Vocabulary. Chapter 701:

	Telecommunications, channels and networks
STN IEC 60050-714 (33 0050)	International Electrotechnical Vocabulary. Chapter 714: Switching and signalling in telecommunications
STN EN ISO 128-1 (01 3121)	Technical Product Documentation (TPD). General principles of presentation. Part 1: Introduction and index
STN EN ISO 128-2 (01 3121)	Technical Product Documentation (TPD). General principles of presentation. Part 2: Basic conventions for lines
STN EN ISO 11354-1 (18 9020)	Advanced automation technologies and their applications. Part 1: Framework for enterprise interoperability (ISO 11354-1: 2011)
STN EN ISO 16484-1 (74 7310)	Building automation and control systems (BACS). Part 1: Project specification and implementation (ISO 16484-1: 2010)
STN EN ISO 16484-2 (74 7400)	Building automation and control systems (BACS). Part 2: Hardware (ISO 16484-2): 2004)
STN EN ISO 16484-3 (74 7400)	Building automation and control systems (BACS). Part 3: Functions (ISO 16484-3:2005)
STN EN ISO 16484-5 (74 7400)	Building automation and control systems (BACS). Part 5: Data communication protocol (ISO 16484-5: 2022)
STN EN ISO 16484-6 (74 7400)	Building automation and control systems (BACS). Part 6: Data communication conformance testing (ISO 16484-6: 2020)
STN EN ISO 17427-1 (01 8610)	Intelligent Transportation Systems Cooperative ITS. Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s) (ISO 17427-1: 2018)
STN EN ISO 17423 (01 8564)	Intelligent Transport Systems. Cooperative systems. ITS application requirements and objectives for selection of communication profiles
STN EN ISO 19650-1 (73 9011)	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Part 1: Concepts and principles
STN EN ISO 19650-2 (73 9011)	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Part 2: Delivery phase of the assets
STN EN ISO 19650-3 (73 9011)	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Part 3: Operational phase of the assets
STN EN ISO 19650-4 (73 9011)	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Part 4: Information exchange
STN EN ISO 19650-5 (73 9011)	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Part 5: Security-minded approach to information management
STN EN ISO/IEC 27019	Information technology Security techniques. Information security controls for the energy utility industry
STN ISO/IEC 7498-1 (36 9615)	Information technology Open Systems Interconnection. Basic Reference Model: The Basic Model
STN ISO/IEC 8822 (36 9633)	Information technology Open Systems Interconnection. Presentation service definition
STN ISO/IEC 8823-1 (36 9634)	Information technology Open Systems Interconnection. Connection-oriented presentation protocol: Protocol specification
STN ISO/IEC 8886 (36 9207)	Information technology Open Systems Interconnection. Data link service definition
STN ISO/IEC 9041-1 (36 9644)	Information technology Open Systems Interconnection. Virtual Terminal Basic Class Protocol Part 1: Specifications
STN ISO/IEC 9646-1 (36 9647)	Information technology Open Systems Interconnection. Conformance testing methodology and framework Part 1: General terms

IEC TS 62443-1-1	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
IEC 62443-2-1	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program
IEC TR 62443-2-3	Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment
IEC TR 62443-3-1	Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

Note: Related and cited standards as amended, including addenda and national annexes.

1.11 Related and cited departmental technical regulations.

[T1]	TS 002	Catalogue of road structures for 115 kN axle load
[T2]	TS 015	General principles for the use of retroreflective road studs
[T3]	TS 016	Catalogue of tunnel defects on roads
[T4]	TS 017	Design of road drainage facilities
[T5]	TS 019	Road construction documentation
[T6]	TS 020	Tunnel terminology
[T7]	TS 029	Road technology equipment, infrastructure and systems
[T8]	TS 030	Intelligent transportation systems and technological transportation devices
[T9]	TS 041	Risk analysis for Slovak road tunnels
[T10]	TS 049	Road tunnel ventilation
[T11]	TS 050	Monitoring of the environmental impact of roads
[T12]	TS 061	Catalogue of bridge structure failures on highways, express roads and Class I, II and III roads
[T13]	TS 066	Determination of noise pollution caused by road traffic
[T14]	TS 069	Use of traffic signs and traffic installations for marking road works
[T15]	TS 070	Forecasting intensities on the road network by 2040
[T16]	TS 076	Monitoring of road bridges
[T17]	TS 080	Road tunnel safety — Safety documentation
[T18]	TS 081	Basic protective measures to limit the effect of stray currents on bridge structures on roads
[T19]	TS 082	Road inspections, maintenance and repair. Tunnels - equipment
[T20]	TS 091	Monitoring concrete tunnel linings
[T21]	TS 092	Road safety management and inspection
[T22]	TS 093	Central control system and visualisation — Tunnels
[T23]	TS 099	Fire safety in road tunnels
[T24]	TS 102	Road capacity calculation
[T25]	TS 103	Transport of overweight and oversized loads
[T26]	TS 115	Road tunnel lighting
[T27]	TS 116	Inspection of tunnels
[T28]	TS 117	Common principles for the use of traffic signs and traffic installations
[T29]	TS 118	Principles for the use of horizontal traffic signs
[T30]	TKP 0	In general
[T31]	TKP 4	Drainage devices and guards for utilities
[T32]	TKP 11	Traffic signs
[T33]	TKP 28	Geotechnical monitoring for tunnels and exploratory shafts
[T34]	TKP 35	Geotechnical monitoring for linear roadway structures
[T35]	TKP 40	Video surveillance and video detection, including ADR — Tunnels
[T36]	VL 2	Road body
[T37]	VL 5	Tunnels

Note: Related and cited departmental technical regulations, as amended including addenda.

1.12 Applicable foreign regulations

[ZP1]	TLS 2012	Technische Lieferbedingungen für Streckenstationen. Bundesanstalt für Straßenwesen Bergisch Gladbach, Bundesministerium für Verkehr, Bau und Stadtentwicklung, 2012, [Technical terms of delivery for stations en-route. Federal Motorway Research Institute, Bergisch Gladbach, Federal Ministry of Transport and Digital Infrastructure, 2012].
[ZP2]	MARZ 2018	Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen, Ausgabe 2018. MARZ 2018, Bundesanstalt für Straßenwesen, Bergisch Gladbach, Bundesministerium für Verkehr und digitale Infrastruktur, [Issue of a Regulation on installations for traffic control centres and subcentres. Edition 2018. MARZ 2018. Federal Motorway Research Institute, Bergisch Gladbach, Federal Ministry of Transport and Digital Infrastructure].
[ZP3]	Datex II	Datex II Exchange data specification. European Commission.
[ZP4]	NTCIP	National Transportation Communications for Intelligent Transportation System Protocol. American Association of State Highway and Transportation Officials (AASHTO) Publications. 2020-2022.
[ZP5]	RFC 2350	Description of CERT-EU.
[ZP6]	IEEE 802.3	IEEE Standard for Ethernet.
[ZP7]	IEEE 802.3.1	IEEE Standard for Management Information Base (MIB) Definitions for Ethernet.
[ZP8]	IEEE 802.3.2	IEEE Standard for Ethernet - YANG Data Model Definitions.
[ZP9]	IEEE 802.3ck	IEEE Standard for Ethernet Amendment 4: Physical Layer Specifications and Management Parameters for 100 Gb/s, 200 Gb/s, and 400 Gb/s Electrical Interfaces Based on 100 Gb/s Signaling.
[ZP10]	IEEE 802.3cs	IEEE Standard for Ethernet Amendment 2: Physical Layers and Management Parameters for Increased-Reach Point-to-Multipoint Ethernet Optical Subscriber Access (Super-PON).
[ZP11]	IEEE 802.3cx	IEEE Standard for Ethernet Amendment 6: Media Access Control (MAC) Service Interface and Management Parameters to Support Improved Precision Time Protocol (PTP) Timestamping Accuracy.
[ZP12]	IEEE 802.11	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
[ZP13]	IEEE 802.11/Cor 1	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Corrigendum 1 -- Correct IEEE 802.11ay Assignment of Protected Announce Support bit.
[ZP14]	IEEE 802.11ax	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN.
[ZP15]	IEEE 802.11ay	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Enhanced Throughput for Operation in License-exempt Bands above 45 GHz.
[ZP16]	IEEE 802.11bd	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Next Generation V2X.

1.13 References

[L1] Road network operations and intelligent transport systems. RNO/ITS manual. PIARC (World Road Association), 2023.
[L2] Intelligent Transportation Systems Technologies. FHWA (Federal Highway Administration), 2022.
[L3] Future of Transport: System interoperability and standards. The British Standards Institution, 2020.
[L4] Ertico announces six priorities to make Europe's transport smarter with ITS at the European Parliament. ERTICO, 2019.
[L5] Reference Handbook for harmonized ITS Core Service Deployment in Europe. Published by Federal Highway Research Institute (BASt), Printed by Federal Ministry of Transport and Digital Infrastructure Division Z 32, In-House Printshop, Germany. Bergisch Gladbach, October 2021.
[L6] Action Plan on Road Transport and Smart Mobility Challenges 2021-2025. Ministry of Transport and Construction of the Slovak Republic, 2020.
[L7] Long-term roadmap for road transport and smart mobility challenges 2021-2030. Ministry of Transport and Construction of the Slovak Republic 2020
[L8] Data models for petrol stations, charging stations for electric vehicles and registration of smart and connected vehicles using the DATEX II standard. Ministry of Transport and Construction of the Slovak Republic, 2022.
[L9] Creation of a detailed procedure (methodology) for the design, integration, deployment and publication of up-to-date information in the area of safe and secure truck parking areas (SSTPA) using the DATEX II standard. Ministry of Transport, 2023.
[L10] D. Littlejohn Shinder, Computer networking essentials, CISCO Press, Softpress, 2003.
[L11] Cybersecurity and information security policy for category I pursuant to Decree No 179/2020 laying down the categorisation method and content of public administration information technology security measures. Ministry of Investment, Regional Development and Informatization of the SR, 2023.
[L12] EU-ICIP, ITS Communications & Information Protocols, CEN/TC 278 ITS Standardization.
[L13] Options for weighing vehicles on highways, express roads and Class I roads, Analysis task, 2020.
[L14] Cooperative intelligent transport systems (C-ITS) Guidelines on the usage of standards, 2020.
[L15] European ITS Platform, chapter 4.2 Physical and digital infrastructure, 2016 – 2021.
[L16] The C-Roads Platform, An overview of harmonised C-ITS deployment in Europe, 2021.
[L17] Support study for the ex-post evaluation of the ITS Directive 2010/40/EU Final report, 2019.
[L18] Final report of the single platform for open road testing and pre-deployment of cooperative, connected and automated and autonomous mobility platform (CCAM platform), 2021.
[L19] The deployment of intelligent transport systems in Europe, Summary of [Z25], EUR-Lex 2023.

1.14 Abbreviations

AID	Automatic incident detection
ASD	Automatic traffic counters
ADP	Traffic flow analysers
API	Application Programming Interface
APV	Application software
BIM	Building Information Modeling
BIOS	Basic Input Output System
OHS	Occupational health and safety
CAV	Connected and automated vehicle Note: [connected, interconnected and automated vehicle]
CCAM	Cooperative, connected and automated mobility

C-ITS	Cooperative Intelligent Transport Systems
CSIRT MIRRI SR	Computer Security Incident Response Team of the Ministry of Investment, Regional Development and Informatization of the Slovak Republic
CRS	Central control system
RTS	Road traffic signalling (road traffic signalling system) [STN EN 50556] or from the term Light signalling devices [TS 019, TS 117, STN 73 6100] – Light signalling system
CCC	Central control room
DSC	Distributed Control Systems
ABD	As-built documentation
E-call	Emergency call, automatic system implemented by vehicle
EESC	European Economic and Social Committee
EN	European standard
EU	European Union
EU-ICIP	European ITS communications and information protocols
EFA	Electric fire alarm (electric fire alarm system)
ESS	Electrical security system (Electrical security alarm system, security system, alarm system)
EUC	Equipment under control STN EN 61508
FAT	Factory acceptance test
GTM	Geotechnical monitoring
HMI	Human machine interface
IACS	Industrial Automation and Control Systems: OT system
ICS	Industrial Control System: OT system
IR	Infrared
IDAM	Identity and Access Management
IED	intelligent electronic device
ICT	Information and communication technologies
IEC	International Electrotechnical Commission
ICC	Integrated control centre
IoT	Internet of Things
IP	Internet Protocol
IPC	Industrial PC; PC with industrial design designed mainly for OT
MIS	Motorway Information System
ISO	International Organization for Standardization
IT	Information technology
IT network	Electrical IT network
IRS	Integrated Rescue System
LAN	Local Area Network
LoS	Level of Service. Note: level (provision) of the service
MaaS	Mobility as a Service

MT	Ministry of Transport
MPQ	Measurement of physical quantities (System of measurement of physical quantities)
MTBF	Mean time between failures
MÚK	interchange
NSA	National Security Authority
LV	Low voltage
PLC	Programmable logic controller
PC (1)	Personal computer
PC (2)	Programmable controller [in accordance with STN EN 61131]
PDI	Physical and digital infrastructure
VTS	Variable traffic signs, markings, traffic signs with variable symbols (STN 73 6100, 3.11.17.3)
MaaS	Mobility as a Service
OT	Operational Technology
CC	Control centre
OPC UA	Open Platform Communications Unified Architecture
PAC	PC-based programmable automation controller
No.	Ordinal number
R	Road(s)
PV	Photovoltaic
PF	Police force
TC	Traffic control
RIOS	Remote input/output station
RCC	Regional control centre (i.e. ICC according to [T22])
AADI	Annual average daily intensities
TCS	Traffic control system
TeCS	Technology control system
RTU	Remote terminal unit, syn. Remote telemetry unit, syn. Remote telecontrol unit
RWIS	Road Weather Information System
RWIS-R	Road Weather Information System for traffic control
SAE	Society of Automobile Engineers
SAT	Site acceptance test
SCADA	Supervisory Control And Data Acquisition
CPS	Central power supply system
SIL	Safety Integrity Level
SK-CERT	Slovak Computer Emergency Response Team
SR	Slovak Republic
STN	Slovak technical standard
TLS	Traffic light signals

ECS	Emergency call stands (Emergency phone stands)
TCP	Transmission Control Protocol
TEN-T	Trans-European Transport Network
TN-C	Terre neutre - combiné [electrical grid with grounded source point. Non-live parts of electrical appliances are connected to this point, the neutral and the protective conductor are merged into a single conductor (PEN) throughout the grid.]
TN-S	Terre neutre - separated [electrical grid with grounded source point. Non-live parts of electrical appliances are connected to this point, protective (PE) and neutral (N) conductors are two separate lines]
ET	Emergency telephones (emergency call system phones)
TS	Technical Specifications
DTR	Departmental technical regulations
UAM	Urban Air Mobility
CCTV	Closed-Circuit Television
VLAN	Virtual Local Area Network [a method used to create logical virtual subnets on a physical network]
VMS	Video management system
HV	High voltage
WAN	Wide area network
WIM	Weigh-in motion

2 Terms and definitions

2.1 Adopted nomenclature

Nomenclature from STN 73 6100 and [Z1] is used.

2.2 Basic terms and explanations

2.2.1 Intelligent Transport System

Intelligent Transport System is a term defined in [Z25], and in a similar way in [Z13]. This term is abbreviated as ITS.

Intelligent transport systems are part of equipment, power and technical facilities of road structures.

These TS address the issue of intelligent transport systems by all the requirements contained in these TS.

These TS also address the issue of C-ITS, which are also intelligent transport systems, in particular in the light of the requirements listed in Article 4.5.14 of these TS and Article 6.1.3.4 of these TS.

The following were issued: [Z26], [Z27], [Z28], [Z29], [Z30], which are essential for intelligent transport systems. AT the EU level, the Reference Handbook for harmonized ITS Core Service Deployment in Europe [L5] was published, which includes a series of guidelines, advice and recommended technical standards and resulting facts that can be used by motorway and road managers and operators to support the development of their strategic approach, the development of the design, deployment, installation and operation of intelligent transport systems and services in a way that is compatible with EU legislation.

Building on related and cited EU legislation, the Ministry of Transport has developed an Action Plan on Road Transport and Smart Mobility Challenges 2021-2025 and a Long-Term Plan to Address Road

Transport and Smart Mobility Challenges 2021-2030 [L6] a [L7] and more specific methodology of data models for petrol stations, charging stations for electric vehicles and registration of smart and connected vehicles using the DATEX II standard[L8] and creation of a detailed procedure (methodology) for the design, integration, deployment and publication of up-to-date information in the area of safe and secure truck parking areas (SSTPA) using the DATEX II standard [L9].

2.2.2 Systems for technical facilities

2.2.2.1 Control system

A control system is a technological system that monitors and controls subsystems and equipment connected to it and configured in it. The subsystem is a subordinate (inferior) system, i.e. a lower-priority system or a lower-level system with a lower management and decision-making privileges in the hierarchy. A system may have a parent (superior) system, i.e. a system with a higher priority or a system placed at a higher level, with higher management and decision-making privileges in the hierarchy. These TS use the terms 'lower-priority system' and 'higher-priority system, others are considered synonymous. These synonyms are found in related and quoted literature.

2.2.2.2 Equipment, power and technical facilities for structures

Pursuant to [Z9], construction works are also assembly works if they incorporate construction products into a structure or remove construction products from a structure in a permanent and fixed manner, in particular operating equipment and equipment, power and technical facilities for structures. The structure connects to the area's public transport and technical facilities.

Intelligent transport systems are also part of equipment, power and technical facilities of roads.

2.2.2.2.1 Technical facilities.

For the purposes of these TS, from the spectrum of equipment, power and technical facilities of road structures, these are higher-priority control systems for HV and LV power installations, control systems for dedicated cable and wireless telecommunications networks, lighting and ventilation systems in tunnels, safety systems, construction monitoring systems, intelligent transport systems, including all their parts and functional elements, and all technical facility systems with higher priority, including second and third-level (and, where appropriate, higher), which for the purposes of these TS are **technical facilities of roads.**

> *Note: from the spectrum of equipment, power and technical facilities, for the purposes of these TS, the following definitions apply:*
> *technical facilities - cables and structural parts of telecommunications networks and all structural design elements of all technical and power facilities;*
> *power facilities — HV and LV power distribution network.*
> *This applies to road equipment and facility structures within the scope of the purpose and use of these TS.*

2.2.2.2.2 Common requirements

We define the term 'Common Requirements' for the purposes of these TS as 'General Conditions and Requirements'.

2.2.2.2.3 Technical facilities. Common requirements.

We define the term 'Technical facilities. Common requirements' for the purposes of these TS as 'General Conditions and Requirements for technical facilities of roads'.

2.2.2.2.4 BIM

As-built documentation for technical facilities will be created in addition to [T5] and Chapter 8 these TS with an optional supplement to as-built documentation created in the BIM system in five dimensions, with three being spatial components, the fourth a timetable and the fifth a budget with a description of items including, in addition to structural items, items for maintenance, technical inspections, repairs and lists of spare parts, instructions for use and operating manuals for the building.

The technical requirements for BIM are given in STN EN 17632 and STN EN ISO 19650-1 to 5. In addition to [T5], the requirements for technical drawings and drawings of buildings follow from STN ISO 128 and STN 01 3420.

2.2.2.3 System element

Each element of a system, whether higher or lower, whether it is a (control) centre, (control) system, control unit, sensor, actuator, component, or element, is also a system in terms of some other conception in the structure of other systems.

2.2.2.4 Hardware architecture

For system elements, within the framework of intelligent transport systems and road equipment, power and technical facilities, for purposes of unambiguous interpretation and identification of the structure, the architecture of centres, systems, control units and functional elements is established. In a road network, there may be several centres that are connected to each other and connected to the main centre directly or through regional centres. The systems consist of a set of connected controllers equipped with processor, memory and communication interfaces. Functional elements are attached to control units. Functional elements are sensors or actuators that are functional in conjunction with the external environment and through the detection of phenomena or human perception. Functional elements sense the state of the environment and road traffic or transmit signals to traffic users. The parts of the system located in the outdoor environment are (outdoor) devices.

2.2.2.5 Software architecture

Because intelligent transport systems are an ICT application, each element of the system at least down to the level of the control unit, in many cases even at a lower level, contains software that ensures its functionality based on a computer program and settings. If, in addition to a processor-executable code, human-readable source text is available via an HMI, it is an open software system. If only processor-executable code is available to the computer program (for the user, customer, client) it is a closed software system. The software system includes settings that can also be open or closed. The control unit and the (digital) computer included in the system contain the firmware and the basic input-output system, which are considered to be components of the device and are usually closed systems. The computer program is executed in the control unit on the central processor unit. For more complex systems, the program is executed through an operating system, which can also be open or closed. The control unit may include connected devices and communication modules, including their driver software. Digital and analogue modules or devices are connected to the inputs and outputs of the control unit to communicate or transmit and adapt signals that are digitised before processing. The computer program collects and processes data and then passes it on. An integral part of the systems together with the computer program are data formats, communication and data protocols, settings, file formats, database structures and APIs. These together form the basic system software. For PLC controllers, the computer program is recorded in the program logic code. Higher-level software for technical facilities, intelligent transport systems, their control systems and higher-priority technical facility control systems is called APV. All this together makes up software configured according to the appropriate specific architecture. For software copyright see Article 2.2.2.6.6 of these TS.

As indicated, the settings can be open or closed. System settings at different levels, from functional elements to control systems and systems with the highest available priority, fundamentally influence the behaviour of software, hardware and thus all road equipment, power and technical facilities of roads. Their identification and specification is available at different levels according to the level of knowledge and skills of internal staff and external experts working with the systems. Records of open settings, like software source code, must be available to the administrator. However, the settings must be protected and hidden from unauthorised persons. Data in the design documentation must be in the non-public part of the design documentation.

2.2.2.6 Copyright and software licenses

2.2.2.6.1 Record of hardware structure and functionality of equipment, power and technical facilities

Hardware structure and functionality are recorded in the form of design documentation. The design documentation is produced in digital form and stored on a digital medium and printed on paper in the required data and print formats.

2.2.2.6.2 Software record

The software is recorded in a computer program that is translated into processor-executable code from source code through a programming language. A computer program is created in digital form and stored on a digital medium or printed on paper in the required data or print formats. Only open-source software programs are printed on paper. In the case of a closed system, only the settings of the system, the computer program and the database are printed.

2.2.2.6.3 Copyright

[Z15] governs the relationships that arise in connection with the creation and use of a copyright work, from the perspective of these TS, in connection with the creation and use of a computer program or database in such a way that the rights and legitimate interests of the author are protected. Copyright does not apply to the text of legislation, an official decision or a court decision, a technical standard, as well as its related preparatory documentation and its translation, and similarly neither does it apply to zoning documentation.

2.2.2.6.4 Copyright supervision and project management

Pursuant to [Z10], an engineer authorised for building equipment, power and technical facilities is authorised to carry out project management, in particular for project management and coordination of sub-projects prepared by engineers and specialists, and to carry out professional copyright supervision over the execution of buildings according to approved design documentation. The engineer performs professional copyright supervision over the execution of buildings according to the design documentation verified by the building authority in the zoning proceedings or building permit proceedings.

2.2.2.6.5 Copyright ownership of design documentation

The owner of the copyright for design documentation will become the client who, through the supply chain, obtained the design documentation from the supplier or contractor of the design documentation under the contract containing the award. The transfer of design documentation copyright must be entrenched in the contract because there is no legislation specifically addressing this issue. Copyright clearance for design documentation is also important from the point of view of possible future changes to the design documentation by an authorised architect or authorised civil engineer other than the one who produced the design documentation. A change in the design documentation may be triggered by various circumstances, including a change in the project by the client.

2.2.2.6.6 Assignment of software copyright

2.2.2.6.6.1 Assignment of copyright for an open software system

For an open software system its content is clear and legible and it is therefore possible to identify the copyrights that pertain to it, and it is then possible, appropriate and necessary, for the author to assign it to a third party via a licence, i.e. from the point of view of these TS, usually to the client. Copyrights of this kind are dealt with in [Z15]. The transfer of copyright, its scope and temporal validity to software, i.e. a computer program that is technically specified, must be enshrined in a contract.

2.2.2.6.6.2 Assignment of copyright for a closed software system

For a closed software system, functionality is identifiable, i.e. functionality based on the way it is used. By selling a license, the manufacturer grants the buyer usage rights. When buying all necessary

licenses, it is important to check the content, completeness, codes, documentation and authenticity. It is necessary to pay attention to the necessary functionality and duration of the licence and to address its renewal well in advance in order to ensure the functionality and availability of the road's equipment, power and technical facilities.

2.2.2.6.6.3 Obligations in the preparation and procurement phase of the project

Pursuant to [Z20]§15(2)(d), in the project preparation and procurement phase, the administrator is obliged to accept the contractual terms according to the obligations set out therein, including the open nature of the source code in accordance with the licensing terms of the public software license under the EUPL [Z37] to the extent that the publication of this code cannot be misused for an activity aimed at disrupting or destroying the public administration information system; it shall be the sole and exclusive holder of all information collected or obtained during the design and operation of the created solution, including its changes and servicing, and when switching contractors, the original contractor shall provide the administrator with full cooperation in switching to a new contractor, in particular in the field of IT architecture and integration. This applies to Article 2.2.2.6.6.1 of these TS and Article 2.2.2.6.6.2 of these TS.

2.2.2.7 Data exchange

Values of quantities converted into values of electromagnetic field quantities, corresponding signals, transformed into data, and vice versa, and the information obtained by their analysis are products of technical facility control systems. Data can also be delivered to ICT from outside through data communication streams and HMI. The data is the property of the administrator, who is obliged to comply with legislative standards when managing them. If it passes them on, out of the system, it must require the same from third parties. For an unambiguous stance on data ownership, it is necessary that the contractor and the customer have the relationship to data ownership clarified in the contract.

The issue of data exchange concerns not only the ownership of the data itself, but also privacy protection, the rules of which are laid down by legislative standards based on [Z35] and [Z36]. The protection of the privacy of individuals and corporate entities must be ensured throughout the process, from data capture, processing and storage, as well as when data is being used. Although the above legislation is mandatory for contractors and the suppliers, due to the clear responsibility in the supply chain and the obligations arising from the use of the data by a third party, it is highly desirable that the relevant relations between the contractor and the customer be dealt with in the contract.

2.2.3 Structure and parts of systems of technical facilities of roads

This article summarises the list of the most used structures and parts of technical facilities of roads (in other words, technological units, technological systems including intelligent transport systems, or E&M equipment for roads [T19]), usually classified as structures for equipment, power and technical facilities of buildings.

Technical facilities are designed, built and operated on a road with a level and scope according to the road's infrastructural importance. Roads with a higher category of infrastructural importance must be equipped with a higher category of technical facilities in order to be capable of operations, see Article 3.3 of these TS. A higher category represents a higher road load and higher requirements for bridges and tunnels that are road structures.

The technical facility systems for roads referred to in this Article, in stage S1 of road power and technical facilities allow traffic on the most heavily loaded loads with infrastructure class V 1.

2.2.3.1 Types of basic systems of technical facilities

The types of basic technical facility systems for roads are as follows:

A. Safety systems

B. Intelligent Transport Systems

C. Structure monitoring systems
D. Higher-priority technical facility systems

The characteristics of basic technical facility systems are in Article 4.5 of these TS.

The list of all technical facility systems is in Article 4.6 of these TS.

2.2.3.2 Equipment in relation to technical facilities

Road equipment in relation to technical facilities referred to in Article 2.2.3.1 these TS includes:
E. Structures and elements

2.2.3.3 Power equipment in relation to technical facilities

Road power equipment in relation to technical facilities referred to in Article 2.2.3.1 these TS includes:
F. HV and LV equipment (gear)
G. Power cables
H. Telecommunications network cables

2.3 Technical terms

2.3.1 Redundancy

In general, smart devices and systems, intelligent transport systems, and road equipment, power and technical facilities can operate when power, networks and the surrounding environment are provided, i.e. the overall environment according to requirements. These requirements must be available for high-reliability equipment and systems without interruption. The way this can be achieved is redundancy in the functioning of all relevant systems.

Redundancy is the deliberate duplication of critical components or functions of a system in order to increase its availability and reliability in the form of backup or failure prevention. In exceptionally important safety systems, some parts of the control system can be triple with a choice of 2 out of 3 or by decision 3 of 3.

Geographical redundancy corrects the vulnerability of redundant devices via geographical separation of backup facilities.

Redundancy must be properly designed so that it does not result in lower rather than greater reliability – to avoid creating an overly complex system that is prone to various problems and malfunctions, which could, for example, lead to neglect of duties by operators or lead to higher manufacturing requirements that could reduce the safety of the system by overburdening it.

In the event of failure of one of the parts of the system, a redundant system continues to function without the need for external intervention and must be able to communicate the failure information to a higher-priority control system.

For redundancy for equipment, power and technical facilities and intelligent transport systems in a more specific breakdown for control units, power units, communication networks and functional elements, see Article 4.1.3 of these TS.

2.3.2 Functional safety

Functional safety is essential to ensure the functionality of each component, member, element, device and system for the operation of a road's equipment, technical and power facilities, including intelligent transport systems. Functional safety is standardised by the STN EN 61508 set of standards to quantify the safety performance of an electrical control system and introduce the concept of a life cycle. The aim is to minimise malfunctions of all electrical/electronic/programmable electronic devices and systems.

The probabilistic approach depends on whether the functional component is exposed to high or low demand requirements. Pursuant to STN EN 61508, high demand is defined as more than once a year and low demand is defined as less than or equal to once a year. For functions that operate continuously (continuous mode) or functions that operate frequently (high-demand mode), SIL specifies the permitted frequency of hazardous failures. For functions that operate intermittently (low-demand mode), SIL specifies the tolerable probability that the function will not respond to a request. The difference between a function and a system is that the system implementing the function may be in operation often, but the function may be requested intermittently. The safety integrity levels (SIL) and their respective discrete values are given in Table 1.

Table 2 Safety Integrity Levels (SIL) and their values

SIL	Low-demand mode, average probability of a hazardous failure	High demand or continuous mode, probability of a hazardous defect per hour
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

The SIL of devices and systems is certified, where a third party confirms that the product, process or system meets the requirements of the certification scheme. Certification programmes for IEC 61508 are operated by impartial third-party organisations called Certification Bodies (CB).

2.3.3 Road section

2.3.3.1 Road section

The road section of a roadway is its part in the relevant direction of traffic, starting at the point of entry on this roadway and ending at the exit. The road section includes the relevant road equipment, power and technical facilities and intelligent transport systems, which are part thereof.

In addition to the road's equipment, power and technical facilities, which are a physical part of the road section, it also includes remote objects on other sections of the roadway, e.g. elements, components and functional members, e.g. traffic management systems and systems outside the roadway. These are primarily a control room, applied telecommunications networks, data and their physical forms used to process, transmit and store information.

The road section includes road equipment, power and technical facilities with a standard level of technical facilities.

2.3.3.2 Technical road section

A technical road section is a road section of a divided roadway with a high level of technical facilities. A technical road section includes road equipment, power and technical facilities and intelligent transport systems of this technical road section, as well as equipment, power and technical facilities of any tunnels or bridges in the road section.

In the case of a technical road section, road equipment, power and technical facilities pertaining to the road section are also installed prior to the entrance to the road section and before the preceding last exit, i.e. as part of the previous section between intersections.

Particular attention is paid to tunnels and bridges and related equipment and technical and power faculties, including intelligent transport systems, and to the equipment they control and that connects road sections.

3 Classification classes, environment and levels of technical facilities and roads

The purpose of the classification for systems, equipment and their elements is to classify them in terms of reliability and availability, impact of the environment and assessing the impact of the environment, external influences in the road environment, and the importance of the road, which

includes both the infrastructural importance of the road and its transport significance. The classification corresponds to the method of use and to the characteristics of technical facility systems and the elements of those systems.

3.1 Reliability and availability

The reliability and availability class determines how strict the requirements placed on system reliability or availability need to be, or on the reliability and availability of road equipment, technical and power facilities. This results in requirements for the immunity of the system and a given component to both internal and external failures and how the component is incorporated into the system in order to achieve system availability. Table 3 defines the reliability and availability classes and their importance in terms of reducing safety during a failure, the consequences of malfunction and the impact of the failure on road operation.

Table 4 Reliability and availability classes for road technical facility systems

Class	Name	Safety reduction during failure	Consequences of malfunction	Impact of failure on road operation
A	high	existing	it is necessary to stop or limit traffic in the road section and it may be necessary to reroute traffic around the road section	system malfunction results in operation being impossible or road operation may need to be limited*
B	standard,	non-existent	no safety reduction	the system is not necessary for road operation

* – limiting traffic in a technical road section is described in greater detail in Table 9.

Classification in reliability and availability classes is based on identification of the degree of safety reduction if the system or equipment in question malfunctions:
1. in the event of failure of a device, on the ability to substitute its function by other means;
2. In the event of a system failure, the ability of active devices to operate safely even in the event of failure of their respective higher-priority system.

> *Note: Degree of safety reduction – corresponds to the term safety deficit. A safety deficit is an element that reduces the safety of a road. Depending on the degree and severity of this reduction, we classify these deficits into three levels for road safety management purposes [Z48], [T21]]. Sections of the road network adjacent to road tunnels of the trans-European road network covered by Directive 2004/54/EC and [Z8] have a particularly high risk of accidents [T21]].*

3.1.1 Road technical facility level

The level of a road's technical facilities determines how strict the requirements put on reliability and availability of equipment, technical and power facilities of the given road need to be, including intelligent transport systems and control room as a whole. The class level of technical road facilities is thus equivalent to the reliability and availability class used for equipment and systems. In the case of technical facilities, it is not possible to evaluate their individual components, and they must be evaluated as a whole for the road section or for the technical road section. Table 5 classifies individual levels of technical road facilities.

Table 6 Definition of technical road facility levels

Level	Name	Description
S1	high	applies to road sections with reliability class A equipment and systems
S2	standard	applies to road sections with reliability class B equipment and systems

The classification level of technical road facilities is specified when designing the equipment, technical and power facilities of the given road, including intelligent transport systems and the control room. Control rooms are assigned to the highest classification level of technical road facilities they operate, i.e. level S1.

The first step is to stipulate the level of technical road facilities. The level of technical road facilities then determines requirements for the reliability and availability class of the technical road facility system.

3.1.1.1 Level S1

Level S1 technical road facilities correspond to the highest levels of transport significance of a road and requires a high concentration of equipment and technical and power systems of the given road, including intelligent transport systems, and the need for communication and power cables along the entire length of a road with this level of technical facilities. In addition, level S1 implies the need for redundant power supply infrastructure, i.e. HV and LV power lines and wiring and telecommunications network cabling and redundancy of control systems. Tunnels with mechanical ventilation, linear traffic control or more than 500 m in length, as provided for in [Z8], must be classified as S1. This Government Regulation regulates the minimum safety requirements for tunnels more than 500 m in length on motorways and Class I roads, in the operation, construction or design phases.

Level S1 technical road facilities belong to the technical road section.

The specific technical solution in terms of redundancy, reliability and availability of
- power supply infrastructure;
- only exceptionally and very partially applied off-grid LV power supply system;
- the telecommunications network;
- control systems;
- higher-priority control systems;
- level two higher-priority control systems;
- control room

is always specified by the design documentation the administrator’s requirements included in it.

The following also needs to be taken into account:
- Article 4.2 of these TS states that in the case of level S1 technical facilities, not all functional elements must meet the requirements set out in Article 4.1.3.4 of these TS. Those that do not must be listed in the approved design documentation;

- Article 4.3 these TS states that in the event of failure of an actuator the control unit must place it in a safe state even in the event of failure of the connection to the control system;

- in the case of level S1 technical facilities, not all control units must comply with the requirements set out in Article 4.1.3.1 of these TS. Those that do not, must be listed in the approved design documentation;

- Article 6.1.2.3.2 of these TS states that the reliability and availability class of a CRS system is specified in Article 6.1.2.3.1 of these TS.

3.1.1.2 Level S2

Level S2 technical road facilities corresponds to medium levels of transport significance of a road, with a low concentration of equipment, technical and power facilities on the road including intelligent transport systems, where there is no need for communication and power cables along the road. Power for equipment and systems is provided using electrical connections found in the given location or from other alternative sources of power. External communication with the control room is provided by own or leased wireless telecommunications technologies or leased telecommunications lines. The technical solution of level S2 technical facilities may be less costly than the technical solution for level S1 technical facilities. However, level S2 cannot be applied when reliability class A equipment and systems requiring redundant communication and power supply are used, or the appropriate redundancy level must be provided by the administrator, e.g. by using third party services.

Level S2 technical road equipment belongs to the road section.

The specific technical solution in terms of redundancy, reliability and availability of level S2 technical road facilities and any redundancy of
- power supply infrastructure;
- any applied off-grid LV power supply system;
- the telecommunications network;
- control systems;
- higher-priority control systems; and
- connection to level two higher-priority control systems and connection to the control room of the technical road section is always given by design documentation and the incorporated administrator's requirements.

3.2 Environmental influence

3.2.1 Climate zone

The climate zone class determines the range of ambient temperature and humidity in which equipment must be capable of permanent operation. Thermal resistance requirements are specified by a combination of environmental class and climate zone class.

Defined climate zone classes correspond to climatic conditions in different localities of the Slovak Republic, and are listed in Table 7.

Table 8 Definition of climate zone classes

Class	Name	Specification by elevation
K1	warm	up to 1000 m above sea level
K2	cold	more than 1000 m above sea level

Where road equipment, technical and power facilities are needed in a cold zone, the contracting authority must specify special durability requirements according to the characteristic local conditions.

3.2.2 Terrain

The terrain class makes functional requirements for structural components associated with equipment and systems (poles, for example) and structural outdoor parts of equipment (cabinets, for example) contingent on the nature of the terrain in which they are installed and the requirements for structural resistance of technical facilities, in particular to wind. Terrain classes are based on its characteristics according to the number and size of obstacles in the terrain, limiting the action of wind and the spread of fog. They take into account the special character of a mountain landscape and narrow valleys as well as built-up areas and the influence of buildings. Terrain classes, if they need to be specified, are based on STN EN 1991-1-3 and STN EN 1991-1-4.

Specific design situations must take into account all loads that can modify the effects of wind such as snow, ice, traffic intensity, traffic speed, etc. Structures that need to be addressed include portals, masts, brackets for mounting devices, construction of cable guards on cornices, snow barriers on

switchboards, racks, stands, etc. These and other requirements are discussed in more detail in Article 5.2 of these TS.
The number of terrain classes that follow from STN EN 1991-1-4, if we do not consider Class 0, which is irrelevant in Slovakia in relation to open sea and seacoast, is 4 (four):
1. lakes or areas with negligible vegetation and without obstructions;
2. areas of low vegetation such as grass and isolated obstacles (trees, buildings) separated by a distance at least 20 times the height of the obstacle;
3. areas regularly covered by vegetation or buildings or isolated obstacles separated
by a distance at most 20 times the height of the obstacle (such as villages, suburbs, permanent forest);
4. areas where at least 15 % of the surface is covered by buildings with an average height greater than 15 m.

3.3 Infrastructural importance of roads

Roads and roads have a transport importance, as they form a road network, transport infrastructure. Pursuant to [Z1], types of roads are defined, according to which roads are divided according to their transport importance, purpose and equipment into:

- motorways;
- roads;
- local roads;
- special-purpose roads.

However, the subject matter of these TS is primarily technical and power facilities of roads, which is represented in the above in only marginal aspects.

For the assessment of the requirements for equipment, power and technical facilities of roads, these TS introduce the term infrastructural importance of a road which applies to technical facilities through transport infrastructure.

The infrastructural importance of a road corresponds to the need to ensure transport accessibility. A road, as part of the road network, is of network importance. The network importance of a road is determined by demand. Demand is AADI.

A road's infrastructural importance determines what functional requirements need to be placed on the system and the overall requirements for the road's equipment, power and technical facilities, including intelligent transport systems, taking into account the absolute intensity of road traffic at the site of their installation. Infrastructural importance is applied in road design as a **basic indicator** for the need to install and build equipment, power and technical facilities for the given road. Classification in infrastructure importance classes is based on the location of the specific equipment and system and an assessment of the annual average of the daily AADI intensities of road traffic at a given road cross-section. Infrastructural importance classes are stipulated on the basis of the current AADI value multiplied by a forward-looking factor for a period of 10 years (according to the column '10-year AADI outlook'; Table 9) or as specified by the administrator (according to the column ‘road with transport importance’; Table 10). Table 11 define classes of infrastructural importance.

Table 12 Infrastructural importance classes

Class	Name	10-year AADI outlook	road with transport importance
V 1	high	greater than 20,000	motorways and selected Class I roads with high traffic intensity specified by the administrator
V 2	low	less than 20,000	roads with lower traffic intensity

The intensities in the table are given as a 10-year outlook for the annual average daily intensities for both traffic directions together. In the case of unidirectional roads, the determined AADI value is doubled before being entered in the table. Class V 1 is relevant for the use of road equipment and technical and power facilities. For class V 2, technical road facilities are used in tunnels pursuant to [Z8] and on road sections, in places designated by the administrator. The proportion of heavy trucks needs to be adequately taken into account.

When designing, implementing and modernising motorways and roads, it is necessary to design and implement equipment, power and technical facilities for structures and intelligent transport systems pursuant to current legislation, technical standards, technical departmental regulations and criteria specified in Table 13.

Table 14 Level of road technical and power facilities – criterion for design, implementation and operation of road equipment, technical and power facilities

Infrastructural importance class	Level of the road's technical and power facilities	Description
V 1	S1	equipment, power and technical facilities in accordance with legislation, standards and TPR pursuant to design documentation approved by the road administrator are necessary for the operation of the road
V 2	S2	equipment, power and technical facilities are needed to ensure increased safety during road operation. The scope is proposed by the design documentation and is approved by the road manager

3.4 Categories, nature and classes of external influences

The categories, nature and classes of external influences are be based on the classification of external influences pursuant to STN 33 2000-5-51.

For the purposes of this standard, areas are divided into the following basic types:
I – interior areas – completely air-conditioned areas
II – indoor areas with permanent temperature control
III – indoor areas with temperature control
IV – indoor areas without temperature control
V – areas under a roof
VI – outdoor areas (places exposed directly to the outdoor climate).

The breakdown into areas I to VI allows a generalised characterisation of certain external influences in the different types of areas to VI by one common class of given external influence (standard external influences). Such a breakdown may in some cases significantly simplify the documentation of externalities.

Regarding the protection of electrical components - see Article 5.1.7 of these TS.

3.4.1 External influence category A – environment

According to this standard the environment is assessed according to the characteristics of the environment itself or by the objects, equipment, etc. are located in that environment.

Category A assesses the following externalities:
AA – ambient temperature;
AB – ambient atmospheric conditions (temperature and humidity simultaneously);
AC – elevation (air pressure);
AD – presence of water;
AE – presence of foreign solid bodies;
AF – occurrence of corrosive substances or pollutants; AG – shocks;
AH – vibrations;
AJ – other physical stresses
AK – the presence of plants and mould;

AL – the presence of animals;
AM – electromagnetic, electrostatic or ionising effects;
AN – sunlight;
AP – seismic effects;
AQ – storm activity;
AR – air movement;
AS – wind;
AT – snow cover;
AU – frost.

3.4.2 External impact category B – usage

External influence category B classes are contingent on the capabilities of persons coming into contact with the electrical wiring and the properties of the substances in the given area.

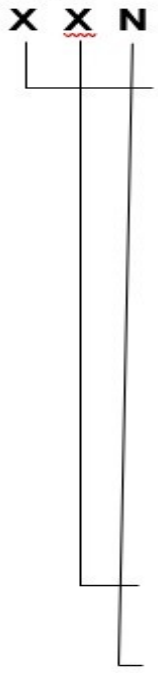
External influence category B assesses the following externalities:
BA – the ability of persons;
BB – the electrical resistance of the human body;
BC – contact of persons with conductive parts at ground potential (touching the ground);
BD – escape conditions in case of danger;
BE – nature of processed or stored substances.

3.4.3 External influence category C – building design

External impact category C is assessed according to the aggregate characteristics of the building or structure (material, construction and installation in the terrain).

External influence category C assesses the following externalities:
CA – construction materials;
CB – building design.

Code



External influence category (letter A, B or C)

A . . . environment
= ambient properties: ambient temperature, humidity, altitude, water, foreign bodies, corrosive substances, pollutants, mechanical stress, flora, fauna, electromagnetic, electrostatic and ionising action, sunlight, seismic activity, frequency of storms, air movement, wind, snow cover, frost

B . . . usage
= characteristics of persons: ability, electrotechnical knowledge, electrical resistance of the human body, number of persons and the possibility of their escape; nature and characteristics of processed and stored substances

C . . . design
= summary of characteristics

Nature of the external influence (letter A, B, C...)

Class (numerals 1, 2, 3...)
= The number of classes for individual types of externalities is different. The interfaces and types of the different classes for the given category and type are defined in the standard in question.

4 Architecture and basic functionality of technical road facilities

As stated in Article 2.2.1 of these TS, intelligent transport systems are part of the equipment, power and technical facilities of structures and therefore the division and layout of a building affects its architecture, and vice versa. A building is divided into structural objects in accordance with construction legislation and design documentation. A structural object usually has an associated technical system assigned to its respective control system. A list of systems by structure and parts is given in Article 2.2.3.1.-3 of these TS. Basic description of structure and description of the architecture of road equipment, power and technical facilities is evident from Article 2.2.2.1.-7 of these TS. The systems include several types of structural components and components of equipment, power and technical facilities of buildings. These components are summarised in Article 5.2 of these TS.

Note: The term 'object' has a general meaning as an object of interest or investigation. An object can be a complex of devices or system elements serving a particular goal. Also used is the term 'object', 'technical object', which can mean a structural object or a general object, which may be part of the equipment, power and technical facilities of buildings.

4.1 Technical road facility systems

4.1.1 Definition of system boundaries

For reasons of appropriate layout of the structure, in terms of TPR, design documentation, implementation of the construction and operation of technical facilities, it is important to establish the boundaries between the technical systems, which define the functionality of the technical facility system and the equipment of the telecommunications transmission network of technical road facilities, cabling of the road's power grid and structural parts and elements. This definition of boundaries addresses hardware interfaces between systems and outside the system. Rules for defining boundaries are specified pursuant to Table 15.

Table 16 Defining boundaries

Subdivision	Group of components	Specific components
is part of the system	functional components	control units, sensor elements, actuator elements
	structural components	switchboard cabinets, building foundations, columns, masts, portals, brackets
	interior wiring	power, electrical and optical telecommunications network cabling equipment and technical elements of telecommunications network equipment
it is not part of the system.	exterior electrical wiring	electrical power cables fed into the equipment switchboard from the outside to the switchboard terminals
	exterior electrical and optical cabling of the telecommunications transmission network	cables of the road's exterior electrical and optical telecommunications transmission network, antennas of the road's wireless exterior transmission network or the public telecommunications network, including supply cables, and technical elements of the exterior telecommunications network to a socket, terminal or interconnection panel
	mechanical protective parts	guardrails, protective barriers

Components of several devices can be placed on a structure, in a switchboard and in a technical switchboard. In this case, it is a shared object. Functional specifications that are part of the design documentation may for such an object, designate one device as primary. All structural and shared

components of such an object are subsequently considered part of the primary equipment. If components of different devices in a single object are interconnected, the corresponding boundary components shall be considered part of the primary equipment.

Pursuant to Article 6.1 of these TS it is clear, however, that establishing a hierarchy through a primary device is not necessary. The point is that the technical facility systems of the road section and the technical road section are designed in such a way that they are virtually separated from each other. For the sake of security, these local area networks are strictly separated and with strictly controlled access. Thus, according to these TS, if no device in the case of a shared object is specified as primary, individual devices shall be assigned to the systems to which they belong. This method is preferred from the viewpoint of these TS.

Note: The term 'equipment' has a general meaning. It can be used to further indicate a set of components connected directly to a control unit.

Technology-construction interfaces, between structural objects, between systems, between sections, are determined by legislation, technical standards and TPR. The precise identification of boundaries always follows and must be clear from the design documentation.

Table 17 Setting the boundaries of a system and a higher-priority system

Is part of a higher-priority control system	Parts of the technical facility control system	Which system it is part of
NO	technical facility switchgear equipment	the relevant technical facility system
NO	telecommunication interconnection switches within a technical road section or a road section	Ethernet LAN of a technical road section (technical part) or of a road section
YES	router equipped with firewall functionality	Ethernet LAN of the CC control room
YES	firewall	Ethernet LAN of the CC control room
NO	firewall between networks of systems with higher priority level 2 and 3	MAN WAN of the regional telecommunications network of the road's technical facility
NO	power grid cables	separate structural object, separate operating complex
NO	electrical and optical cables of the telecommunications transmission network	separate structural object, separate operating complex

In the case of Table 7 and Table 8 this is about the definition of hardware boundaries. Software interfaces specify relevant control systems and higher=priority control systems.

Identifiers in design documentation, software and visualisation are governed by the provisions of [T22] in the section on the principles of labelling of technical facilities in CRS software. These identifiers help to identify the hardware and software boundaries of the technical facility systems of roads.

4.1.2 Electrical switchboards

We distinguish the following electrical switchboards
1. HV and LV, power switchgear, are part of electrical power wiring; and
2. Switchgear for technical facilities

Electrical switchgear is protected by appropriate placement and from a structural design perspective must meet the requirements of Article 5.2 of these TS.

If necessary, electrical switchgear is equipped with heating, ventilation, cooling, sunshades, snow barriers, and protection against damage and theft.

On divided roads at the location of the planned traffic corridors, secondary RX electrical switchboards for powering portable road signs for marking work in progress will be built in the middle belt. Each secondary RX switchgear includes two single-phase TN-S single-phase service sockets with nominal 230 V AC power and a 16 A circuit breaker.

Each main, each secondary switchboard, each off-grid LV power distribution system and each technical switchboard must include two single-phase service sockets of the TN-S single-phase system with a rated alternating voltage of 230 V and a circuit breaker of 16 A.

The reliability and availability class of switchgear within technical road section is always A.

The reliability and availability class of switchgear within the transport section if this is not linked to any technological transport section is B.

In the case of interconnection between a road section and a technical road section, it is recommended that switchboards and switchboards of the road technical facility system ensuring the diversion of traffic from the technical road section are of reliability and availability class A. However, this must be designed at the request of the administrator in the approved design documentation.

4.1.2.1 HV switchgear

High-voltage switchgear, HV switchgear is part of the power facilities and are specified according to STN EN 62271-200, STN EN 62271-201, STN EN 62271-202 and STN 61558. For more details, see Article 5.1 of these TS.

4.1.2.2 LV switchgear

Low-voltage switchgear, LV switchgear, is specified according to STN EN IEC 61439, STN 61557 and STN 61558.

LV switchgear is part of the power facilities. It can be main or secondary and its characteristics are described in Article 5.1 of these TS.

4.1.2.3 Switchgear for technical facilities

Switchgear for technical facilities is part of technical facility systems Their design is subject to STN EN IEC 61439. Technical facility switchgear cabinets contain technical facility equipment and systems located outside the control centre building.

Low-voltage electrical installations for equipment, technical and power facilities of structures on a road are designed, implemented and operated in accordance with the STN 33 2000 group of standards.

Components of technical facilities intended to be placed in switchgear, where possible and appropriate, must be designed for switchgear with a 19" inner frame width and are placed directly into the inner frame of the switchgear. Alternatively, smaller components must be designed to fit on a DIN rail and shall be mounted on a DIN rail.

Technical facility switchgear cabinets situated on a foundation on the ground or on the walls of structures must be designed to enable installation both on 19" inner frames and on DIN rails.

Switchgear cabinets located on columns may be smaller and designed to allow only DIN rail mounting.

Switchgear for technical facilities of a technical road section with level S1 technical and power facilities, intelligent transport systems and level 2 or 3 higher-priority control systems, in terms of functional safety characterised pursuant to Article 2.3.2 of these TS must comply with at least safety integrity level (SIL) 2.

Switchgear shall be designed and implemented according to design documentation approved by the administrator based on the relevant and valid STN.

4.1.2.4 Required signals from switchgear

The basic signals from switchgear for technical facilities of a technical road section intended for the relevant system, a higher-priority system and the relevant CRS as a system with a higher priority of level 2, are at least as follows:
- opening the switchgear door;
- failure of any control unit contained in the switchgear, including camera failure;
- loss of power.

A detailed specification of the signals is given in [T22].

4.1.3 Redundant equipment, power and technical facilities

4.1.3.1 Redundant control unit

A redundant control unit is a device of reliability and availability class A consisting of at least two mutually cooperating control units that outwardly represent the functionality of a single control unit.

4.1.3.2 Redundant power supply

A redundant power supply is a device of reliability and availability class A consisting of at least two power supplies. Its system shall ensure that the failure of one of them does not cause the power supply as a whole to fail. If this unit is equipped with a rechargeable battery it is a UPS, i.e. an uninterrupted power supply.

4.1.3.3 Redundant communications network

A redundant communications network is a network in which, in the event of failure of one of its components (active element or cable connection), mutual communication remains possible. A redundant communications network must also be physically redundant, i.e. communication between any two nodes is guaranteed even if all components of one switchgear unit are physically destroyed, including the interruption of all cable connections. A redundant communications network is part of a level S1 technical facility system.

4.1.3.4 Functional elements of reliability and availability class A

Reliability and availability class A sensors must be implemented as intelligent functional members and must be connected exclusively to reliability class A control units, i.e. redundant control units. They must be connected to the control unit via a redundant communications network – an intelligent process bus pursuant to STN EN IEC 61131-9. Data exchange between programs is pursuant to STN EN IEC 61131-10. Sensor elements of reliability class A must have redundant executive blocks – each quantity must be measured by two independent executive blocks and the measured values must be independently transferred to the control unit. If they do not match (outside the allowed value tolerance and time shift) the measurement is faulty. Alternatively, the mismatch may be evaluated directly in the sensing element: the measurement value is transferred to the control unit only if the measurement is assessed as correct. Reliability and availability class A actuator elements must be implemented and connected in the same way as reliability class A sensors and the same rules apply to feedback measurement.

The executive block ensures the essence of the function of the given functional element. In the case of sensors, it is a sensing element that responds to a physical, chemical or other similar phenomenon, usually by changing its electrical (conductive) properties, which are subsequently recorded by the control unit. In the case of actuator elements, this is an element that reacts to a change in its electrical properties, elicited by a command from the control unit, by changing its or surrounding physical, chemical or other similar properties. An intelligent functional element can contain multiple executive blocks (associated functional element).

Redundant equipment, power and technical facilities are used for level S1 technical facility systems on a technical road section. For a broader and more general explanation of the term redundancy, see Article 2.3.1 of these TS. Redundancy is an important characteristic of equipment, power and technical facilities as well as of intelligent transport systems themselves. The general requirements should be adequately reflected in the approved design documentation, implemented in construction and maintained in operation.

General requirements for functional elements are set out in Article 4.2 of these TS.

4.1.4 Tunnel technology

Tunnel technology (equipment, power and technical facilities of road tunnels) is a separate sub-group that is dealt with special legislation, standards, literature and TPR [almost everything on the list]. The same is true of bridges. Increased risks are present, which are proportionate to the increased care of the road manager and the State, and hence there is also an increased concentration of intelligent transport systems and other systems containing equipment, technical and power facilities. Tunnels and bridges on a road with an infrastructural importance class V1 and level S1 road equipment, technical and power facilities contain an entire spectrum of equipment, technical and power facilities, including intelligent transport systems, that are essential for their operation. For road tunnels and bridges with class V2 infrastructural importance and level S2 road equipment, technical and power facilities, this spectrum is narrowed.

The basic task of tunnel technology is to create safe conditions for traffic in the tunnel, identify any incident, and help address the situation.

In terms of traffic flow, there is no distinction between roads, bridges and tunnels.. The requirements for traffic safety and compliance with traffic regulations are the same everywhere.

If a CRS at the tunnel level, a safety system or any intelligent transport system, a higher-priority system at the ICC level detects information that makes it unsuitable or safe for vehicles to be in a tunnel, on a technical road section or on a road section, it must be capable via a TCS, either automatically or via an operator, to close the tunnel, technical road section or road section, i.e. prohibit the entry of vehicles thereinto. Until the situation is resolved, equipment, power and technical facilities, including intelligent transport systems, must continue to behave in such a way that they inform drivers that they should allow the police and the integrated rescue system to do their work and assist competent personnel during the evacuation of vehicles and people from tunnel, technical road section or road section. A more detailed and comprehensive context is set out in [T22] a [T23].

4.1.5 Bridges and interchanges

Bridges on a road section, a technical road section and within an interchange are located in complicated positions, often in urban environments and branches the interchange can also intersect tunnels. A traffic incident or structural collapse may lead to situations where it is necessary to take measures such as those referred to in Article 4.1.4 of these TS.

Bridges therefore need to be adequately equipped with equipment, technical and power facilities and intelligent transport systems, the scope and use of which are proposed by the design documentation and approved by the road manager.

Bridge reflex matrix – the inter-reaction of equipment, technical and power facility systems of a bridge and the CRS of the technical road section is in Table 9 Technical road section CRS reflex matrix.
Further to Article 4.1.4 these TS, on a road with infrastructural importance of class V1 and level S1 road equipment, technical and power facilities, an entire spectrum of equipment, technical and power facilities, including intelligent transport systems on bridges, are essential for their operation. A summary of this equipment relating to bridges is given in Table 9. Each bridge with a length greater than 500 m or a length as determined by the road manager must be so equipped. We call such a bridge a mandatory bridge, and analogically a tunnel with level S1 equipment, technical and power facilities a mandatory tunnel. If there is more than one mandatory bridge or mandatory tunnel in a technical road section technical facilities operate integrally, i.e. all reflexes are manifested identically along the entire length of the technical road section. In areas before the first mandatory bridge or the first mandatory tunnel, there must be sufficient space to create a traffic restriction based on the traffic signs specified in the approved design documentation and the approved road sign designation.

CRS integrates reflexes for all mandatory bridges and mandatory tunnels in a technical road section. For CRS behaviour, the same rules apply to the technical road section as for tunnel reflexes. Their description and the requirements to be met are given in [T22].

As regards the road's telecommunications network, the activity of CRS in terms of safety, reliability and availability is characterised in Article 6.1.2.3.2 of these TS.

Table 18 CRS reflex matrix for a technical road section

Information, status	Standard operation	HV and LV	Lighting	ET	ET	CCTV
	Operation without restrictions	Failure	Failure	Activation	Failure	Failure
Activation						
Structural monitor	In operation	On	On	On	On	On
Lighting at night	In operation	Off	-	On	On	On
ET lighting	In operation	On	On	Flashing	On	On
TS lighting	In operation	On	On	On	On	On
ET	In operation	On	On	Communicating	-	On
CCTV	In operation	On	On	Activation	On	-
AID	In operation	On	On	On	On	On
TCS and VTS	In operation	On **	Restriction	Restriction	On	Restriction***
CRS	In operation	Alarm	Alarm	Alarm	Alarm	Alarm

Information, status	AID	AID	TCS	VTS	Structural monitor	Structural monitor
	Failure	Detection.	Failure	Failure	Failure	Detection.
Activation						
Structural monitor	On	On	On	On	On	On
Lighting at night	On	On	On	On	On	On
ET lighting	On	On	On	On	On	On
TS lighting	On	On	On	On	On	On
ET	On	On	On	On	On	On
CCTV	On	On	On	On	On	On
AID	-	-	On	On	On	On
TCS and VTS	Restriction***	Restriction	Closure *	Restriction***	Restriction***	Closure *
CRS	Alarm	Alarm	Alarm	Alarm	Alarm	Alarm

* – closure of technical road section, activation of traffic exclusion from a section and activation of a detour, do not enter and red light on all VTS and RTS, where possible

** – restriction at night

***- in case of VMS server failure (CCTV) or AID or structural monitor (in case of a long-term failure lasting more than one day)

****- operator activity according to the decision of a police officer

For the closure of the technical road section, see also Article 4.4.2.1 of these TS and 4.4.2.2 of these TS.

4.2 Functional elements

Functional elements are sensors or actuators that are directly connected to the external environment. They are placed according to their purpose, either in switchgear, on the road (invasive elements) or on support structures.

The minimum general requirements for functional elements are as follows:
1-connectivity to the control unit;

2-functionality given by the manufacturer in a location designated for it in a road environment;
3-compliance with the parameters given by the manufacturer in climate zone K1 in the temperature range from -15 °C to + 40 °C;
4-also function outside the temperature range specified in point 3.

In the case of level S1 technical facilities, not all functional elements must meet the requirements set out in Article 4.1.3.4 of these TS. Those that do not must be listed in the approved design documentation.

The full range of technical requirements beyond the above-mentioned minimum general requirements for specific functional elements is set out in the TPR that applies to the relevant issue or in the approved design documentation.

4.3 Control units

A control unit, in cooperation with the control system, must meet the following minimum general requirements:
1-recognise whether a functional element is working properly and is connected;
2-provide the control system information in case it or the functional element malfunctions;
3-collect data through functional elements and provide it to the control system;
4-transfer the control system's signals to functional elements;
5-if an actuator malfunctions, place it in a safe state even in the event of failure of the connection to the control system.

In the case of level S1 technical facilities, not all control units must comply with the requirements set out in Article 4.1.3.1 of these TS. Those that do not, must be listed in the approved design documentation.

The full range of technical requirements beyond the above-mentioned minimum general requirements for specific functional elements is specified in the relevant TPR that deals with the relevant issues from the point of view of a particular control system (a summary of control systems is in Article 4.4.2 these TS, characteristics in Article 4.5 of these TS) or in the approved design documentation.

4.4 Control system

4.4.1 Basic characteristics of road control systems

A basic explanation of the terms for understanding the nature and level of road control systems is given in chapter 2 of these TS.
A view of the basic architecture and structure of road control systems is in Article 2.2.2.4 of these TS, and 2.2.2.5 of these TS.

Links between authors and creators with the administrator and buyer of control systems is in Article 2.2.2.6 of these TS.

Products of control systems, signals and data, their description and the basic contexts of their origin and use are listed in Article 2.2.2.7 of these TS.

The structure and parts of technical road facility systems, types of basic technical facility systems, structural monitoring systems and higher-priority technical road facility systems are summarised in Article 2.2.3 of these TS.

4.4.2 Road control system levels

Each basic system of equipment, technical and power facilities, such as HV and LV power equipment, power cables, electrical and optical telecommunications transmission networks, technological elements of the telecommunications transmission network, ventilation in tunnels including air MFQ in tunnels, tunnel lighting, video system, ASD, ADP, WIM, VTS, RTS, RWIS, fire alarm system, security alarm system or any other not mentioned here, has its own, basic road control system.

Basic control systems are linked to a higher-priority control system. Higher-priority control systems are AID, MIS, TCS, TCS, TCS and potentially others not listed here.

Note: If we use the term 'higher-priority control system' in these TS, it is a general statement or a control system with a higher priority of the first level, to which individual basic control systems are connected and internally interconnected. We do not use the adjectives 'basic' and 'first degree' for the sake of simplicity and conciseness of the text, only if needed for the sake of clarity and context. Specifically it also concerts this article, where we distinguish control systems, i.e. explain their levels.

A higher-priority control system means a higher-level control system. A lower-priority control system means a lower-level control system. In terms of CRS and ICC visualisation systems, a higher-priority control system is allowed to have a full overview of all lower-priority systems.

CRS connects and connects AID, MIS, TCS, RTS and directly connects and interconnects or can connect and interconnect other basic road control systems from the above list. It is a SCADA system and is controlled by the CC's HMI. CRS is a level 2 higher-priority control system. CRS controls equipment, power and technical facilities of a technical road section and other higher-priority control systems of adjacent technical road sections and road sections.

The ICC connects and interconnects several CRS, i.e. level 2 higher-priority control systems. The ICC is therefore a level 3 higher-priority control system. The features of the ICC are explained in more detail in Article 4.4.4 of these TS.

As explained in Article 6.1 these TS and its sub-articles from the perspective of a telecommunications network, for the needs of roads in Slovakia, under certain circumstances level 3 higher-priority control systems may be sufficient. If not, a higher level may be required: level 4.

A summary of the basic levels of road control systems and respective control system levels is as follows:
A. **control system** (basic road control system), is a system belonging to a specific device, e.g. ASD or VTS and RTS (light signals)

B. **higher-priority control system** (level 1 higher-priority control system) for example, this is the system of an individual ASD to the ASD of the manager; TCS

C. **level 2 higher-priority control system**, which is CRS

C. **level 3 higher-priority control system**, which is ICC

In order to identify systems with a higher priority, the design documentation must include at least the following information:
A. control systems – a list of all systems applied, list of objects, descriptions;
B. higher-priority control system – a list of individual control systems assigned to it, descriptions;
C. level 2 higher-priority control system - characteristics, description;
D. level 3 higher-priority control system to which a level 2 control system will be assigned.

4.4.2.1 Fire mode

In accordance with [T22], for selected defined devices (in accordance with the matrix of automatic tunnel reflexes and the corresponding design documentation), it is possible to activate the fire control mode. This primarily concerns equipment that affects the progress of fire and the progress of evacuation. In this mode, the equipment's technical and electrical protections and protection logic are automatically deactivated and lower-priority remote control modes are also suppressed (automatic, manual and forced). In fire mode, the equipment must be manually controlled without restrictions. The fire control mode is activated and deactivated manually by authorised control room personnel on the instruction of the commander of the firefighting operation.

4.4.2.2 Technical road section closure mode

Closure of a technical road section pursuant to Article 4.1.5 of these TS, in the event of a failure of the TCS or a detection recorded by the structural monitoring system, is analogous to and inherently also includes this mode. In this mode, the equipment's technical and electrical protections and protection

logic are automatically deactivated and lower-priority remote control modes are also suppressed (automatic, manual and forced). In technical road section closure mode, the equipment must be manually controlled without restrictions. The technical road section closure mode is activated and deactivated manually by authorised control room personnel on the instruction of a police officer.

4.4.3 Requirements for road control systems

4.4.3.1 Requirements for basic control systems

A control system must ensure that the following minimum functional requirements are met:
. controlling control units connected to the system;
. collecting data from all control units;
. data processing;
. data distribution;
. data storage;
. managing communication with databases;
. data export;
. controlling equipment and processes;
. communication in the process network;
. optionally, basic data visualisation through an HMI;
. the ability to operate via the control unit and its service interface – the relevant control unit is controlled;
. the ability to control via a higher-priority control system – all control units are controlled.

Equipment belonging to control systems of a technical road section with level S1 technical and power facilities, level 2 and level 3 control systems, in terms of functional safety characterised according to Article 2.3.2 of these TS must comply with at least SIL 2.

4.4.3.2 Requirements for a higher-priority control system

This is a control system with level 1 higher priority In addition to the minimum functional requirements referred to in Article 4.4.3.1 of these TS, it must be capable of facilitating:

. implementation of the systems and equipment assigned to it through the CC;
. access by employees – operators to the control system through an HMI;
. comprehensive control of lower-priority systems;
. connection and interconnection to a system with level 2 higher priority;
. all relevant requirements arising from [T22].

> *Note: MIS is a control system level 1 higher priority , to which individual basic control systems outside of tunnels on the road section are connected and internally interconnected. MIS is used to indicate a structure. The MIS does not need to be equipped with a CC.*

If it is equipped with a CC (control centre), then

. the CC must meet ergonomic requirements;
. displays must be capable of displaying a video stream from a video system by means of a VMS;
. it must be able to receive and display alarms from connected systems by visualisation;
. it must allow alarms to be handled in accordance with the operating manual.

4.4.3.3 Requirements for a level 2 higher-priority control system

This is the CRS control system. It is described and the requirements are set out in [T22].

The CRS control system has a three-layer architecture in terms of software, where the individual layers correspond to the basic types of tasks performed:
1. communication layer – ensures communication with devices and functional elements of all connected and interconnected systems;
2. application layer – provides data processing, client access and process control;
3. visualisation layer – ensures the visualisation of data and the performance of system management by the operator.

4.4.3.3.1 OT CRS

It is an industrial ICS control system that comprehensively concludes the OT part of the system. It is an electronic control system with related hardware and software used to control industrial processes. Control systems can range from several panel-mounted modular controllers to large interconnected and interactively distributed DCS control systems. Control systems receive data from remote sensors that measure process variables, compare the collected data to the required values, and derive command functions that are used to control the process through end control elements, actuators. Larger such systems, such as intelligent transport systems and equipment, power and technical facilities of road structures, DCS and PLC networks are integrated SCADA systems. SCADA is used to integrate all lower-priority systems into the CRS control system. When designing and building a higher-priority system and control system IT, the STN EN 62264 group of standards is applied, for designing and building a CRS EN 61175-1 and the STN EN IEC 61131 group of standards.

4.4.3.3.2 Integration of systems in CRS

CRS is a system integrating individual ICS for road equipment, power and technical facilities and intelligent transport systems of a technical road section and are dedicated to it [T22]. These [T22] are developed for the purpose of updating and amending existing legislation for the design and implementation of technical facilities of road tunnels, adjacent parts of motorway sections and relevant road sections, focusing on the technical solution for CRS and visualisation system. TS [T22] define minimum requirements for the functionality and parameters of the CRS central control system, the visualisation system and the technical facilities of the road tunnel from the point of view of automated control. TS define the way APV controllers and visualisation system are created in terms of functionality, scope and form.

4.4.3.3.3 CC

CC, described in more detail in [T22], is a system that enables control of CRS or ICC, i.e. control of road equipment, technical and power facility control systems, including intelligent transport systems, through systems level 2 and 3 higher priority through operators' HMIs. From the point of view of the telecommunications network, the CC is characterised in Article 6.1.2.3.1 of these TS.

The CC (control centre) of a road section, technical road section or region, is an operations centre for operators operating equipment, power and technical facilities of a road through operator's positions, with significant user of visualisation methods on a SCADA software platform intended for the control and coordination of traffic, and, if required, to ensure communication between operating personnel and other stakeholders.[T19]

The CC is designed, built and operated in the road manager's building.

A specific CC must be designed and built in the context of the relevant higher-priority system according to the design documentation approved by the administrator. Operation and maintenance must be subject to strict rules according to the operating manual, the building manual, the organizational rules, and the rules of information and cyber security.

4.4.3.3.4 CRS and ICC

The control and visualisation architecture specified in [T22], from the perspective of local and remote control, in addition to an adequate description of the structure and functionalities of the system and of the relevant components, defines the operator positions, operator positions for temporary control, emergency control and integrated operator positions for multiple tunnels and the regional operator position. Due to the required redundancy of systems, there is also a need for a backup ICC.

As a level 2 higher-priority control system, CRS integrates higher-priority control systems and within them, or directly, all control systems for road equipment, technical and power facilities.

From the point of view of the telecommunications network of a technical road section, the CRS is characterised in Article 6.1.2.4.2 these TS and from the point of view of the arrangement of telecommunications interconnection of systems with level 2 and 3 higher priority in Article 6.1.2 of these TS.

Individual CRS, as control systems with a level 2 higher priority, can be integrated into the ICC, as control systems with a level 3 higher priority. See also Article 4.4.4 of these TS.

4.4.4 ICC

Just like the aim [T22] to unify the principles of control and the appearance of visualisation from the point of view of the operator, so that the technical and personnel integration of the control of individual tunnels into the regional tunnel control rooms for tunnels (RTCC/ICC), or subsequently into a central control room (CCC) it is necessary to ensure integration of equipment, technical and power facility systems and intelligent transport systems on all road sections and roads for the reason referred to in Article 4.1.4 of these TS that 'in terms of traffic flow, there no distinction is made between roads, bridges and tunnels'.

The minimum requirements for ICC solutions for the integration of equipment, technical and power facility systems and intelligent transport systems on all roads include:

• requirements for structures and parts of systems and control systems with higher priority and control centres necessary for their integration into a higher ICC level;

• requirements for technical solution of interconnections of control systems with higher priority and control centres according to DATEX II standard, see Article 6.1.2 of these TS, and 6.1.3 of these TS;

• requirements for APV and the ICC visualisation system;

• there is a need for backup ICC.

Individual CRS, as control systems with a level 2 higher priority, can be integrated into the ICC, as control systems with a level 3 higher priority. See also Article 4.4.3.3.4 of these TS.

4.4.5 TCS

A traffic control system (TCS) is one of the level 1 higher-priority control systems when it comes to the direct implementation of road traffic management through basic intelligent transport systems pursuant to Article 4.4.5.1 of these TS;

TCS in transport applications pursuant to Article 4.4.5.2 of these TS belong among control systems with a higher priority of higher levels. In this case, this is regional and supplementary exercise of control.

A TCS is a subsystem of control systems with a higher level higher priority.

Controlling traffic using traffic operating conditions and controlling traffic using traffic signs and traffic equipment is possible only based on the instructions of a competent police officer.

4.4.5.1 Traffic control (TC) through Intelligent Transport Systems

A TCS performs control through the functional elements of intelligent transport systems, VTS and RTS, and must therefore be connected to devices implemented in the form of signalling cross-sections and traffic equipment:
a) VTS (variable traffic signs);
b) signs with operational information and network control panels;
c) signal lights.
A TCS participates in the traffic control process as described in Article 2.2.1. of these TS, and 4.1.4 of these TS and others.

A TCS uses data and information obtained on a given road section by all available systems from those listed in Article 2.2.3.1 these TS, and 2.2.3.2 of these TS, systems with higher priority and decide automatically or through operator intervention.

A TCS performs TC pursuant to [T8] with the exception of the rules laid down in 4.1.4 of these TS, and 4.1.5 of these TS.

Traffic control methods and the TCS itself may be designed, implemented and operated only on the basis of approved design documentation and approved traffic conditions.

The minimum requirements for VTS and RTS are set out in EN 12966+A1 STN EN 50556 and STN EN 12368, and also in the relevant legislation and standards listed in them.

The use of VTS, RTS, retro-reflective and active illuminated road studs as traffic light signal systems is also described in [T28] [T2] and STN EN 50556 and the legislation, standards and TPR mentioned therein.

4.4.5.2 Traffic control application via C-ITS

For the purpose of facilitating the provision of compatible, interoperable and continuous real-time traffic information services across the European Union, road authorities, road operators, service providers, in-vehicle information holders and recharging and refuelling stakeholders shall provide real-time network usage data collected in DATEX II format (the STN EN 16157 group of standards and subsequently updated versions, or in an alternative manner, see Article 6.1.3.2 of these TS) within the meaning of [Z31]. For the purpose of providing appropriate information directly to end-users and optimisation of traffic management and road safety, road authorities and road operators may request in-vehicle data holders and service providers to provide types of data on the use of the network in real time.

Traffic control through intelligent transport systems and C-ITS at the level of regions and larger geographical wholes, or with the support of modes other than road transport, shall be implemented according to the methodology and procedures set out in [L5]. For road managers and operators and road networks, the exchange of data and information enables the provision of transport information and TC (transport control) services.

The specification of services provided by Intelligent Transport Systems is given in the following areas:
1. Functional and organisational interoperability with neighbouring service providers;
2. A uniform appearance and impression on the presentation of basic ITS services to the end-user;
3. Accurate provision and acquisition of information on national access points and C-ITS interfaces;
4. EU-wide accepted criteria for the evaluation of basic ITS services (e.g. quality level).

The methodologies and procedures are defined by:
- road administrators and operators;
- service providers;
- end users;
- Member States.

4.5 Characteristics of technical road facility systems

4.5.1 CCTV

Characteristics of CCTV as a camera video system in the field of safety systems, intelligent transport systems in the context of a road's equipment, technical and power facilities is listed in [T35] including the necessary specifications of individual technical solutions, assumptions and principles for carrying out tests, inspections, maintenance and repairs. During operation it is necessary to apply [T19].

4.5.2 ASD, ADP and WIM

A basic requirement is measurement of the relevant quantities within the defined tolerances and metrological requirements and the provision of output based on the classification of vehicles according to traffic composition specified in [T24]. Given the international dimension of transport and traffic in Europe, it will be appropriate, for reasons of data compatibility and interoperability, to consider updating the adaptation of classification classes. The development of sensors and detectors that may be invasive or non-invasive with respect to roads is ongoing and will continue.

Technical specification of ASD and ADP is provided in [T8], partial specification of WIM is provided in [T8] and a detailed description and extended WIM specification are provided in [L13].

4.5.3 RWIS

The required RWIS properties are specified in [T8] and the STN EN 15518 group of standards.

Weather stations connected to RWIS, TCS as well as stations connected to both RWIS and TCS systems must always meet the minimum requirements of reliability and availability Class B technical facility systems. Class A is not required for weather stations even in the case of an TCS with class S1 technical facilities.

4.5.4 AID

The technical specifications for AID are in [T8].

4.5.5 Ventilation in tunnels

The design, implementation and operation of ventilation systems in road tunnels in the Slovak Republic are subject to [T10]. During operation, [T19] applies.

4.5.6 Tunnel illumination

The design and verification of lighting parameters in road tunnels related to traffic safety applicable to any tunnel or underpass in which lighting needs to be installed shall be carried out according to [T26]. During operation, [T19] applies.

4.5.7 EFA

The design, implementation and operation of electronic fire alarm systems is carried out pursuant to the STN EN 54 group of standards in accordance with [T23] and [Z8].

4.5.8 ESS

Electronic security systems are designed, built and operated in accordance with [Z41] a [Z42]. Private security is operated as a private security service or as a technical service for the protection of property and persons. The operator of the security service and the operator of the technical service are kept in the records of contracts for the provision of security services and in the records of contracts for the provision of technical services.

4.5.9 ET

The emergency telephone system available on roads in ECS and in tunnels in SOS cabins is designed, built and operated according to [Z25] and STN 73 6101.

4.5.10 GTM

Geotechnical monitoring for tunnels and exploratory shafts is carried out pursuant to [T33] and geotechnical monitoring for objects of linear parts of roads is carried out pursuant to [T34].

In the case of construction, data and evaluations from the system belong to the builder, the investor and, in the case of operation, the administrator who is responsible for the relevant follow-up actions directly or through contractual partners. This statement applies appropriately to data from all systems pertaining to a road's equipment, power and technical facilities.

4.5.11 Limiting the effects of stray currents

The effects of stray currents on road bridges are characterised and limited pursuant to [T18].

4.5.12 Monitoring of bridges

Road bridges are monitored pursuant to [T16].

4.5.13 Traffic infractions and strict liability

The application of strict liability for infringements of selected road traffic rules will increase the safety of road users while ensuring that road users are disciplined and respectful by enforcing compliance in particular with those provisions. [Z3]as a result of road accidents resulting in death and bodily injury. In accordance with the current version of the Act, the Slovak Police Force has the means of ensuring

compliance with road safety through strict liability. Currently, the Police Force is the only entity authorised to apply strict liability for infractions in the road transport sector.

4.5.14 The C-ITS technical standard

This article lists the basic selected requirements via references to chapters of Specification [L12]. If there are related technical standards for each chapter, they are listed there.

4.5.14.1 Intelligent Transport Systems

Definitions, requirements and explanations of all intelligent transport systems and some of their characteristics, that are beyond the scope of the specifications of basic control systems and higher-priority control systems in these TS but are applicable under European legislation, are in Chapter 1 and Chapter 6.

4.5.14.2 Architecture

The architecture of intelligent transport systems is presented in Chapter 7.

4.5.14.3 Communications and interfaces

Communications and interfaces of intelligent transport systems are presented in Chapter 8.

4.5.14.4 CCAM, CAV and C-ITS

CCAM, CAV and C-ITS systems are in Chapter 9.

4.5.14.5 Freight transport

Freight transport and the use of intelligent transport systems by freight carriers are listed in Chapter 12.

4.5.14.6 Automated mobility along road shoulders

Automated mobility along road shoulders and kerbs, especially in towns and villages, is characterised in Chapter 13.

4.5.14.7 Local authorities and data

The relationship with local authorities and authorities, data and responsibilities is characterised in Chapter 14.

4.5.14.8 Portable and mobile devices

Mobile and portable devices for Intelligent Transport Systems services are designed to facilitate the development, development and standardisation of the use of mobile and portable devices to support the provision of Intelligent Transport Systems and multimedia services, such as passenger information, car information, driver advice and warning systems, entertainment system, interfaces linked to ITS service providers and motor vehicle communication networks. The standard supports the introduction of mobile equipment in public transport and cars. Mobile and portable devices for Intelligent Transport Systems services are specified in Chapter 23.

4.5.14.9 Parking

Parking is addressed in Chapter 16.

4.5.14.10 Public transport

Public transport is characterised in Chapter 17.

4.5.14.11 Rail transport

Rail transport and information for multimodal use are in Chapter 18.

4.5.14.12 Traffic data and geographic applications

Traffic data and geographic applications from all systems and maps are in Chapter 19.

4.5.14.13 Traffic control

Traffic control, TCS, information provision and related technical standards are listed in Chapter 21.

4.5.14.14 Warning and control

Vehicle warning and control systems are addressed in Chapter 24.

4.5.14.15 Application of standards

A more detailed explanation for application is given in [L14].

4.5.14.16 Physical and digital infrastructure, PDI

C-ITS and CCAM use PDI, parts of which are distributed according to Table 19 PDI attributes. The interdependence of infrastructure and systems must be respected in the case of road equipment, power and technical facilities.

Table 20 PDI attributes

Attribute	Physical/digital infrastructure	Static/dynamic
road	physical	static
speed range	physical	static
shoulder or kerb	physical	static
horizontal traffic markings	physical	static
vertical traffic signs	physical	static
technical road facilities	physical	static
traffic	-	dynamic
time	-	dynamic
weather conditions	-	dynamic
high-resolution map	digital	static
satellite localisation	digital	static
means of communication	digital	static
information system	digital	static
traffic control, TC	digital	dynamic
infrastructure maintenance	physical/digital	dynamic
fleet surveillance	digital	dynamic
road network digital twin	digital	dynamic

PDI attributes are assigned pursuant to [L15]. The reason for compiling these attributes is to enable highly automated driving (SAE level 4) and to assign these attributes to the requirements of automated vehicles to the road infrastructure.

The parts of road infrastructure, power infrastructure, equipment and technical facilities according to these TS comply with the attributes given in Table 21.

4.5.14.17 Deployment of intelligent transport systems - current status

The deployment of intelligent transport systems, including CCAM and C-ITS, in testing and mainstream applications in Europe is proven. The results of testing the application of the latest technical specifications can be found in the literature, e.g. [L16], [L17], [L18] and [L19].

4.6 List of technical facility systems

A summary list of technical road facilities is provided in Table 22. The names of the listed objects are based on the content and context listed in Chapter 4 of these TS.

Table 23 List of technical facility systems

No.	Name
1	Camera video systems and CCTV
2	ASD, ADP, WIM and detailed measurement of vehicle attributes
3	RWIS and MFQ
4	AID

5	Ventilation
6	Lighting
7	EFA
8	ESS and other (not specified) security systems
9	ET
10	GTM
11	Stray currents
12	Traffic infractions and strict liability
13	C-ITS external systems, C-ITS information systems, other (not mentioned here) intelligent transport systems
14	TCS
15	CRS
16	CC
17	ICC
18	Portable and mobile C-ITS devices, provision of traffic information
19	Integrated transport system
20	Static traffic and parking guidance systems
21	Systems with higher priority than CRS and ICC

Technical facilities include active technical elements of technical and power facilities. A list of systems of technical elements of equipment and power facilities is provided in Table 24, which is a continuation Table 11.

Table 25 List of technical facility systems for equipment and power facilities

No.	Name
22	Active technical elements of structures and building elements
23	Active technical elements of telecommunications networks
24	Active technical elements of power networks

Content and links with monitoring systems for structures, ventilation and lighting – see Chapter 4 of these TS.

Content and links with a road's telecommunications and energy networks – see the subsequent Chapter 5 these TS and Chapter 6 of these TS.

4.7 Operation

Road equipment, power and technical facilities are mainly operated through a control centre, CC.

The principles of control and the appearance of visualisation from the point of view of the operator so that technical and personnel integration of control is possible are given in [T22].

4.7.1 Operating records

All systems must keep operating records of individual events on an ongoing basis. Operating records must be stored and archived exclusively electronically, and access to these data must be reserved only for users with special system administrator privileges.

Operating records must be recorded in separate files. These must be in text file format with UTF-8 encoding, where each row contains a single event record and must contain at least the following data:
1. the date and time of the event;
2. the severity of the event: critical, error, warning, notification, information, debugging record;
3. identification of the module (process);
4. the name and description of the event.

The system must make a record of each event, and must make it possible to set the range of records that will actually be recorded and which ones will be ignored. It must be possible to adjust the filtering according to the modules (processes) and for each of them individually according to the severity of the event.

Operating records must be rotated automatically by calendar months. Automatic rotation must ensure the removal of operating records set to more than 3 months old, unless otherwise specified by the approved design documentation.

4.7.2 Operational and crisis procedures

Within the scope of requirements for documentation pursuant to Article 8.1 of these TS, it is necessary to process operational and crisis procedures for the use of road equipment, power and technical facilities.

4.8 Summary of common requirements for technical facility systems

4.8.1 In general

Intelligent Transport System – inform traffic users, ensure a more coordinated use of transport networks, ensure smooth traffic and use of transport networks with maximum safety

- AID system – provide traffic incident data
- ASD, ADP, WIM and detailed measurement of vehicle attributes – to provide individual vehicle data and comprehensive traffic flow data
- Camera surveillance and video system – monitor the road and traffic on it
- Security systems, including camera surveillance, video system and AID – monitor the road and associated area, provide information on its breach, provide information and presence of vehicles and persons, including during evacuation of the area if possible
- RWIS and MFQ – provide information on road and atmospheric conditions
- Ventilation and lighting – allow the use of the road and allow evacuation as far as possible
- TCS – based on the inputs from the subsystems and instructions of a competent police officer, to control traffic using operational traffic states and to control traffic using traffic signs and traffic devices
- CRS – control all systems of technical facilities on the road section and automatically close the road section based on evaluation of tunnel reflexes
- Higher-priority control systems – exchange data and information, control relevant lower-priority systems

All road equipment, technical and power facility systems – with the support and control of higher-priority systems must create the safest possible space for the smoothest possible traffic on the road while complying with environmental requirements.

4.8.2 Design

See Chapter 8 of these TS.

4.8.3 Implementation

The implementation of technical road facility systems is based on legislation, technical standards, TPR and the rules set out in this Chapter 4 of these TS.

4.8.4 Operation and maintenance

The operation and maintenance of technical road facility systems is based on legislation, technical standards, TPR and the rules set out in this Chapter 4 of these TS.

5 Power supply infrastructure and structural elements

5.1 Power supply infrastructure

The p supply infrastructure provides the supply of electricity from external sources to the equipment, technical and power facilities of road structures, including equipment, systems and control centres of technical road facilities.

The power supply infrastructure represents the HV and LV electrical power distribution grid. The power supply infrastructure must be designed, implemented, tested and operated according to valid STN. The technical requirements of these activities are defined in particular by the set of electrotechnical standards of class 33 and 34, the which represents minimum requirements for power supply infrastructure.

5.1.1 The HV and LV power distribution grid

The power supply infrastructure consists of the following parts:
1. external power sources
    a) the public distribution network
    b) central power supply systems (CPS) in the sense of STN EN 50171
    c) motor generators
    d) other alternative sources of electricity

(Note: A CPS is a central power supply system that provides the required power in case of emergency to essential safety devices without limiting their output power.)

2. the electrical distribution system
    a) HV or LV connections – IT network (HV) or TN-C (LV);
    b) separate electrical switchgear – TN-S network;
    c) main power wiring – TN-C network.

The main power wiring ensures the transmission of electricity from external sources to the power supply units of objects (main and secondary switchgear). Separate electrical switchgear are power sources for individual technical objects.

HV switchgear is specified pursuant to EN 62271-200, STN EN 62271-201 and EN 62271-202.

LV switchgear is specified by the STN EN IEC 61439 set of standards.

Internal electrical wiring within technical objects that powers individual technical facilities are not considered to be part of the electricity supply infrastructure. The interfaces between the power infrastructure and technical objects are explained in Chapter 4 of these TS. In this case, technical objects refer to the distribution frames belonging to technical road facilities containing components of technical road facility systems and equipment. The electrical supply infrastructure, i.e. LV power wiring, ends at terminals in distribution frames of technical road facilities.

Electrical connections and main power wiring are implemented using aluminium core cables, all other wiring in the TN-S system with copper core cables.

5.1.2 Power categories

The relevant classification class, see Chapter 3 of these TS, the degree of redundancy and technical standards specified in this article determine the reliability and availability of power infrastructure, its connection and the choice of power sources.

The reliability and availability of an external power supply represents the category of power supply and the level of security of the power supply.

The power supply category and security level are addressed by the design documentation according to the importance and required safety in the sense of STN 34 1610 in three levels:
1. Level – power from two independent sources, where the failure of one power supply does not result in a power interruption. The power supply may be uninterrupted or with interruptions according to operating conditions,
2. Level – two different sources (other substation, transformer, diesel generator), switching can be automatic (short-term) or manual (long-term) and is associated with a power supply interruption.
3. Level – no other source available.

5.1.3 Off-grid LV power supply system

If parts of road equipment, technical and power facilities are
A. significantly distant from public power lines,
B. no HV and LV power lines were run to them during road construction, a power supply solution outside the public distribution network will be used: an off-grid LV power supply system. Off-grid LV power supplies are either:
c) motor generators or
d) other alternative sources of power.

If PV (photovoltaic) systems are used as alternative sources of power, STN 33 2000-7-712 is applied.

The STN documents referred to in this Article apply to the distribution of electricity from the main switchgear to secondary switchgear and to technical facility distribution frames, or for the distribution of electricity from the main switchgear to the switchgear(s) of the LV off-grid power supply system technical facility as if the LV power supply system had been connected by an LV electrical connection from the public distribution grid.

5.1.4 Cable routes

In the architecture of the power distribution system of technical road systems, there are several special power supply routes. The following Table 26 defines these routes

Spatial, mechanical, electrical and fire protection aspects taking into account the effects of the environment are important for the quality of cable routes.

Table 27 Power cable routes

Power route	Purpose	Requirements
power supply cables	power supply from an external source to the main switchgear	if the external source is the public LV distribution network with a three-phase TN-C system, the cable has 4 wires; if the external source is a CPS with a three-phase TN-S system, the cable has 5 wires
main power cables	distribution of electricity from main switchgear to secondary switchgear	
secondary power cables	distribution of electricity from secondary switchgear to technical facility distribution frames	if a three-phase TN-S system is applied, the cable has 5 wires; for single-phase TN-S system, the cable has 3 wires
local power cables	distribution of electricity from an off-grid LV power supply system technical facility distribution frames	same as for secondary power cables

5.1.5 Routing and installation of cable routes

Power cables are routed pursuant to STN 73 6101 and STN 73 6102. On motorways, power or telecommunications cables can be placed in auxiliary plots of land, in a lateral dividing strip or in an unpaved shoulder, exceptionally in the median strip. The term auxiliary road lots is defined in [Z1]. These auxiliary road lots are managed by the road administrator and the width of these strips are determined by the competent road administration within the limits of the implementing legislation.

More precisely, according to these TS, power or telecommunications cables are laid along the road on the right, in the direction of chainage, in a common power cable trough along with telecommunication cables, separated from each other so that they do not affect each other mechanically or electromagnetically. If there is a drainage pipe in the vicinity, it should be installed vertically lower so as to avoid flooding the cables if possible. Individual power cables are placed in conduits or under cover plates. Telecommunication cables are placed in HDPE conduits. An inspection cable shaft is located every at least 1000 m and in its location a transverse connection is made to the opposite side of the road under the road body to a secondary switchgear, where telecommunication cables are also terminated if they are not connected. Cable routes are routed between the main LV and secondary LV switchgear, between secondary LV switchgear and secondary LV switchgear and technical facility distribution frames. A technical facility distribution frame may also act as secondary switchgear. Any cable, even unconnected, must be terminated in the appropriate switchgear on the designated terminals.

The spatial arrangement of technical facility cabling, cable conduits in common trenches and cable routes is specified in STN 73 6005.

Cable routes technical facility level S1 are in redundant configuration along the entire technical road section. In the case of a tunnel, the cable routes in redundant connection run under the sidewalk in

both the right and left tunnel tube, or in cable troughs on the walls or below the ceiling in technical areas, cable shafts are located at least at each transverse connection and at the tunnel portals. In the case of a bridge, in rooms or on both right and left outer cornices of right and left bridges, always accessible and visible in special metal conduits made of non-corroding material, supported on special brackets of non-corroding material.

The required lifetime of cable routes, in particular cables, brackets and conduits, is at least 30 years, or a different lifetime required by the administrator.

Cable routes for level S2 technical facilities may run along the entire road section or along defined sections where necessary, or an off-grid LV power supply system is used. Route location will be specified by the administrator in design documentation.

The precise routing and placement of cables, their joining, splitting and termination, the location of shafts and switchgear must be designed, constructed and operated according to design documentation prepared pursuant to the STN listed in this Article 5.1 of these TS and approved by the administrator.

5.1.6 Continuous power supply during fire

Fire safety of equipment, power and technical facilities of road structures from the point of view of permanent power supply in the event of fire must comply with STN 92 0203.

5.1.7 Degree of protection provided by enclosures, invasive sensors

Enclosures, IP code, the degree of protection of an enclosure for road equipment, power and technical facilities must, based on the environmental class specified pursuant to Article 3.4 of these TS must comply with STN EN 60529. In this respect, the most demanding applications for roads are invasive sensors, i.e. sensors that are installed in the surface layer of the road in such a way that they come into contact with the external environment. Where possible, non-invasive sensors should be prioritised, which is more progressive in terms of maintenance and expected service life, but may not be the case in terms of accuracy of the measured parameters. For invasive sensors, minimum IP 67 protection is required.

5.1.8 Electromagnetic compatibility

Components and parts of systems of road equipment, technical and power facilities must comply with electromagnetic compatibility requirements pursuant to [Z46] and STN EN 50293.

5.2 Structural elements

Structural elements of equipment, technical and power facilities of road structures, including Intelligent Transport Systems, are those parts associated with equipment and systems that enable them to be placed in a space and protect them physically and against weather or an aggressive road environment, including tunnels, bridges, underpasses and overpasses. They are therefore the following:
— (external) enclosures: cabinets housing electrical switchgear or technical or telecommunications switching equipment;
— (external) supporting structures: columns, masts, portals, brackets, support structures attached to walls, ceilings, beams and various other structural elements. The requirements do not apply to structures and components installed in the control centres in buildings, but apply to their corresponding parts located outdoors.

In addition to classifying the appropriate location of the design, installation and operation of the equipment and system into a terrain class, see Article 3.2.2, it is also necessary to assess relationships to STN EN 1991 on actions on structures (group of standards), to the related Eurocodes (groups of standards), namely STN EN 1990, which determines the principles and requirements for the safety, usability and durability of structures, describes the principles for their design and verification and provides guidance on the related aspects of the reliability of structures;
STN EN 1991-1-1 outlines the design procedure and loads for the design of building and civil engineering structures, including some geotechnical aspects for the volumetric weight of building and stored materials, the inherent weight of structures, the utility loads of buildings; STN EN 1991-1-3

provides guidance on the determination of snow loads to be used in the design of building and civil engineering structures; STN EN 1991-1-4 provides guidance for determining the wind load in the design of building and civil engineering structures; Other relevant groups of standards are STN EN 1992 Design of concrete structures, which specifies, inter alia, the principles for the design of structures made of plain concrete, reinforced concrete and prestressed concrete; STN EN 1993 Design of steel structures; STN EN 1994 Design of composite steel and concrete structures; STN EN 1996 Design of masonry structures; STN EN 1997 Geotechnical design; STN EN 1998 Design of structures for earthquake resistance, STN EN 1999 Design of aluminium structures and relevant parts of the above standards 1-2 loading of fire-stressed structures and structural fire design. Other required characteristics from the perspective of fire safety are listed in [Z8], [T23] and [Z45].

For specific structures, their load-bearing parts and foundations, the design documentation must contain a drawing of the structure, a static drawing, a static calculation and, if applicable, a static assessment.

The covering and support structures shall be placed in such a way that no part or part of the equipment fitted to them interferes with the clearance cross-section with the margin given by technical standards and legislation.

On a road with infrastructural importance of class V1, the location of the covering and support structures must allow access to them from a point located outside the road, but if this is not possible, at least from the shoulder and the extended shoulder where a service vehicle can be parked so that it does not interfere with the driving lane. Safety for employees performing installation and service work and road traffic are significantly positively affected by this factor.

Covering structures must be designed, implemented and operated in such a way as to be protected against water by suitable positioning or drainage and against impact using physical barriers. Passive safety of structures designed, implemented and operated in the immediate vicinity of the road must be ensured by road restraint systems pursuant to the EN 1317 group of standards and related TPR.

5.3 Summary of common requirements for power supply infrastructure and structural elements

5.3.1 Power supply infrastructure. Common requirements – summary

5.3.1.1 In general

The power supply infrastructure supplies electricity from external sources to the equipment, technical and power facilities of road structures, including equipment, systems and control centres of technical road facilities.

5.3.1.2 Design

Basics assumptions – see Chapter 8 of these TS.
The power supply infrastructure must be properly designed, implemented and operated in the first place pursuant to the STNs listed in 5.1 of these TS.

5.3.1.3 Implementation

The implementation of the power supply infrastructure is based on legislation, technical standards, TPR and the rules listed in Article 5.1 of these TS. The power supply infrastructure must be properly implemented according to the STNs listed in Article 5.1 of these TS.

5.3.1.4 Operation and maintenance

The operation and maintenance of the power supply infrastructure is based on legislation, technical standards, TPR and the rules listed in Article 5.1 of these TS. The power supply infrastructure must be properly operated according to the STNs listed in Article 5.1 of these TS.

5.3.2 Structural elements. Common requirements – summary

5.3.2.1 In general

Structural elements of equipment, technical and power facilities of road structures, including Intelligent Transport Systems, are those parts associated with equipment and systems that enable them to be placed in a space and protect them physically and against weather or an aggressive road environment, including tunnels, bridges, underpasses and overpasses.

5.3.2.2 Design

Basics assumptions – see Chapter 8 of these TS.
Structural elements must comply in particular with the safety and static requirements set out in Article 5.2 of these TS.

5.3.2.3 Implementation

The implementation of structural elements is based on legislation, technical standards, TPR and the rules set out in Article 5.2 of these TS.

5.3.2.4 Operation and maintenance

The operation and maintenance of structural elements is based on legislation, technical standards, TPR and the rules set out in Article 5.2 of these TS.

6 Road telecommunications network and cybersecurity

6.1 Road telecommunications network

6.1.1 Road telecommunications networks

Road telecommunications networks provide data transmission within a road's equipment, technical and power facilities. Data transmissions perform communication between OT systems, control units, between various systems, between certain devices, communication within process networks, transmission to control systems and to higher-priority control systems, or their mutual communication, transfers for the needs of IT administrators, the ability to connect to the administrator's contractual partners, interconnection with C-ITS, transmissions for IT systems of the police, fire and rescue, a national system with higher priority 3 or 4, intelligent transport systems, MaaS, interconnection to international intelligent transport systems, mobility and MaaS systems, and interconnections to the it systems of road administrators of various infrastructural and transport importance.

The Electronic Communications Act [Z43] states that 'Every newly built building and building undergoing reconstruction of internal wiring for which a building permit is required must be equipped with high-speed physical infrastructure in the building and an access point. The provision of high-speed in-building infrastructure and an access point is considered a general technical requirement for the design of buildings pursuant to a special legislation.'

Pursuant to [Z43] network operator means a network provider or entity operating or providing a network intended for the operation of road infrastructure.

Telecommunications networks of technical road facilities are networks set out in Article 6.1.2.1 these TS, including LAN control centres (CC). These networks must comply with the requirements set out in [Z43].

6.1.2 Design of the road telecommunications network structure

The structure of the road's telecommunications network depends on the structure of the road's equipment, technical and power facilities, which in the case of these TS corresponds to the purpose of road's equipment, technical and power facilities. The purpose of the road's equipment, technical and power facilities corresponds to the structure of the general requirements for technical facilities.

No network access points of the 'technical node' type shall be applied. Network technical solutions must exhibit flexibility, the required data transmission rate, response time, manageability associated

with diagnostics and security of the communications network. **A specific solution is always given by approved design documentation.**

A new design, pursuant to these TS, is compatible with the previous type thanks to the application of international standard IEEE 802.3.

6.1.2.1 Arrangement of telecommunications interconnection of technical facility systems of roads

Arrangement of telecommunications interconnection of technical facility systems of roads is based on the current state of affairs so that it corresponds with [T22]. Control system of a technical road section with level 2 higher priority does not correspond entirely with the interpretation of the term LOP used in the past. The point is that a control system of a technical road section with level 2 higher priority may be connected to a relatively large number of LANs of other road sections and technical road sections. Their basic specifications ire given by the level of technical and power facilities, which pursuant to Article 3.1 of these TS levels can be at level S2 and S1. These levels correspond to the class of infrastructural importance, which is a basic indicator of the need to build equipment, technical and power facilities for the given road.

Telecommunications networks are divided into

1. **regional telecommunications networks for technical road facilities**, which are basic telecommunications networks,

and

2. **telecommunications networks for road sections**, as well as telecommunications networks technical road sections.

6.1.2.2 Regional telecommunications network for technical road facilities

A regional telecommunications network for technical road facilities is therefore a network composed of several LANs of individual road sections or road section networks grouped into a regional network operated by the ICC and connected to the IT network of the relevant road network administrator.

The regional telecommunications network is built along the entire length of motorways (including expressways) in parallel with the motorway network of the Slovak Republic and represents the interconnection of level 3 higher priority control systems and the ability to connect with the network of the relevant road network administrator, other administrators and third parties.

The relevant parts of the regional telecommunications network of technical facilities have IT or OT design depending on which parts and interfaces are defined in the design documentation and how. More detailed breakdowns and contexts are determined by the administrator, in particular for reasons that follow from Article 6.2 of these TS.

6.1.2.3 Road section telecommunications network

The telecommunications network of a road section consists of a telecommunications interconnection within the road section, its control systems, process networks and higher-priority control systems such as a LAN based on the IEEE 802.3 international technical standard.

The telecommunications network of a road section is always in an OT type, up to and including level 3 higher priority control systems.

> *Note: due to the definition of a road section in Article 2.3.3, the above attributes also apply to a technical road section.*

6.1.2.3.1 CC

A CC is designed, built and operated in the administrator's building at the technical road section or technical operations structure or at another location where it is possible to connect to the telecommunications network of the technical road section. However, if this desirable from a geographical point of view or from the point of view of other needs, the CC may also be built by the

road section. Each CC requires its systems to have a CRS, i.e. a control system with a level 2 higher priority. However, in the case of only a road section, at least one higher priority control system may be sufficient, e.g. a VMS, TCS or some other road equipment, technical and power facility systems, including intelligent transport systems, that would be integrated into the higher priority control system. Every road administrator builds a CC for its OT system for technical road facilities of various infrastructural and transport importance according to its needs based on design documentation and relevant legislative processes, see Article 6.1.1 of these TS. The interconnection of IT and OT networks must [comply with?] the provisions of Article 6.2 of these TS. The functionalities of the CC are described in Article 4.4.3.3.3 of these TS.

The reliability and availability class of a level 2 higher-priority control system, i.e. CRS, and the OT system for a technical road section is A.

The reliability and availability class of a higher-priority control system and an OT system for a road section if this is not linked to any technical road section is B.

6.1.2.3.2 CRS

The central control system (CRS) of a technical road section is a level 2 higher-priority control system and integrates all lower-priority control systems. The integration includes the interconnection of OT networks and IT.

From a safety point of view, the CRS must provide tunnel reflections [T22]but also actions (reflections) in the event of bridge collapses or other catastrophic events on the relevant road section or in its immediate vicinity (e.g. an emergency situation in an industrial complex located near the road section). The CRS will do this through its integrated lower-priority control systems connected to the OT network. The technical road section CRS reflection matrix is set out in Article 4.1.5 of these TS.

The CRS contains the necessary systems, such as the operator trainer, the creation of reports for the administrator, calculations and data collection for the integrated transport system, data archiving, etc., and systems providing computing power for all other road equipment, technical and power facility systems.

Because as a level 2 higher-priority control system, the CRS integrates all lower-priority control systems, it must operate on a redundant basis in 24/7 mode.

The availability of visualisation is also ensured through the displays of operators' client workstations and the OT emergency control system. SCADA and its respective servers have a physical separation of pairs of redundant servers at least and proportionately according to the spatial capabilities of the administrator pursuant to Article 2.3.1 of these TS.

The reliability and availability class of the CRS system is stipulated in Article 6.1.2.3.1 of these TS.

The telecommunications network of the technical road section must ensure all minimum requirements pursuant to [T22]. The exact scope for a specific solution results from the design documentation approved by the administrator.

6.1.2.3.3 Operator HMI

Client workstations with operator HMI devices are redundantly connected to the SCADA system servers. The OT includes redundantly connected separate parts of OT emergency control and OT temporary control, which contain a visualisation touch panel. Due to possible failure of the visualisation system, or due to the need to perform technical intervention, this is connected to enable independent emergency control directly and independently from the main SCADA visualisation servers to the process networks and through them to the functional members of the control systems of the technical road section, which require actions of tunnel reflections.

6.1.2.3.4 Higher-priority control systems

The CRS contains the main control parts of higher-priority systems, which together form one whole through integration into the CRS. Higher-priority systems are connected to **all** technical facility systems of the road section or technical road section. The APV of these and/or other higher-priority

control systems is linked to the CRS, which has superior position as a level 2 higher-priority control system. CRS is made up of the APV of the SCADA control system, which bears responsibility for integration.

The distribution of the CRS server system is performed on the basis of the design documentation according to the LAN structure, the assignment of individual control systems to the individual VLAN sub-networks, the APV structure and the appropriate performance that will provide hardware capacity specified by the design documentation. The hardware capacity reserve must be at least 50 %.

6.1.2.3.5 Technical road section control systems

Technical facility control systems are connected to higher-priority systems via a LAN. Systems are made up of connected control units in sub-networks. Communication hardware – switches and hubs, control units – PLC, PC, PAC, DSC and IPC, are located in technical facility switching frames. K-type network topology or other topology specified in the non-public part of the design documentation is used.

In order to determine the characteristics of the control systems of technical road section technical facilities, it is essential to determine the reliability and availability of systems and system elements, such as equipment, control units and parts thereof, in particular, in the case of this Article, their communication interfaces, the characteristics of the functional elements and the characteristics of the relevant process networks. Compliance of characteristics, in particular with regard to the CRS, must be ensured pursuant to [T22].

Communication interfaces of control systems and all higher-priority systems of the technical road section are divided into two basic groups:

1. Communication interfaces of control units that provide key operational and safety functions must fulfil class A reliability and availability requirements. Reliability is given by the correct functionality, redundancy, automatic diagnostics and a MTBF parameter value of the redundant control unit communication interface in accordance with [T22] of at least 20 years. From the communication point of view of the control system and its availability, a redundant control unit consists of at least two interconnected and cooperating control units, making up what from the outside looks like one functional whole. Failure of one control unit, its communication interface, must be automatically diagnosed and the functionality of the redundant unit as a whole must continue to be ensured by other control units without operator intervention.

2. Communication interfaces of control units meeting class B reliability and availability requirements. In terms of reliability, MTBF, it is up to the designer to decide which communication interface system of the control unit will be selected in agreement with the administrator and no redundant connection is required in terms of availability.

The control systems of a technical road section are equipped with interfaces with class A reliability and availability with a redundant connection. However, some functional elements, according to the design documentation, may have simple, non-redundant connections, their communication interfaces are sufficient in class B reliability and availability.

6.1.2.3.6 Interconnection of control systems and their process networks

The connection of distributed PLC I/O modules and DSC PC control units within the OT network to the redundant control unit must be implemented in a redundant manner at the system level of the control system used.

To ensure communication redundancy of the main control unit with decentralised modules of the DSC network a K-topology technical road section OT network and OT process networks or another topology specified in the non-public part of the design documentation.

LAN communication networks must be separated for IT systems and OT systems. Each communication network must be separated from other networks by a firewall.

Access points to the telecommunications network of technical road sections for functional elements, control units and technical road facility systems are implemented by means of switches connected to the telecommunications network of technical facilities.

The functional elements and control units of equipment shall be connected to the access point via a hub using an H connection. H topology reduces the possibility of network failure by connecting to the central node. Use of H topology or another topology is specified in the non-public part of the design documentation. Each component communicates with the other via the central node. Failure of the connection between a component and the central node will only cause the component to fail and thus isolate it from other components and control units.

Data transmissions between the control unit and functional elements are considered to be part of the relevant equipment and in the past they were not considered part of telecommunications infrastructure. However, these are process networks, which create a significant part of telecommunication interconnections. (In some cases, there are significant distances between the control unit and the functional elements, e.g. in tunnels, where control units of technical facilities such as ventilation or lighting are located in a technical room and the functional elements belonging to these control units are distributed over the entire length of the tunnel).

6.1.2.3.7 Means of communication

Means of communication are as follows:

1. the communications cable and structural system:
   a) technical facility distribution frames;
   b) telecommunication wiring;

2. active network elements designed to carry out data transmissions:
   a) firewalls;
   b) routers;
   c) switches;
   d) hubs;
   e) communication interfaces of control units; and
   f) signal converters (transducers).

In the past, the communication interfaces of controllers, functional elements, higher priority systems, or internal communication lines within facilities were not considered independent means of communication. However, these are parts of process networks. They become part of these networks at the moment of connection when they begin to affect communication on the network. The control units are PLC I/O, other PCs, IPCs or PACs that are part of systems controlling sensing or actuator functional elements.

The communication cable and structural system and the active network elements designed to carry out data transmissions form the elements of the telecommunications infrastructure system. A road telecommunications network can only be a system unambiguously designed in the relevant design documentation, drawn up and approved in accordance with procedures under the Construction and Telecommunications Act and also implemented according to this design project documentation.

The overdesign margin for means of communication must be at least 50 %.

The margin must be recalculated proportionally on the basis of a specific technical solution. Additional requirements are determined by the road administrator.

6.1.2.3.8 Ethernet LAN

Within a technical road section, telecommunication interconnection of technical facilities is carried out through a **LAN** designed, built and operated according to the IEEE 802.3 standard and its respective set of standards. In an Ethernet LAN, all systems, the control room, parts thereof and control systems with higher priority are connected in the local network and, as far as possible, controllers and functional elements too. The LAN of a technical road section will also enable wireless connectivity via

the IEEE 802.11 standard, always exclusively via encrypted connection. For all types of connections and interconnections via the LAN of a technical road section, cybersecurity rules apply according to Article 6.2 of these TS.

The operation of an Ethernet LAN is specified for selected operating speeds from 1 Mbps to 400 Gbps using a common specification for media access control (MAC) and management information base (MIB), which is a database used to manage entities in a communication network. The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol specifies shared half-duplex traffic as well as fully duplex operation. Speed-specific Media Independent Interfaces (MII) enable the use of selected Physical Layer (PHY) devices to operate via coaxial cables, twisted or optical fibre pairs or electric motherboards. Multisegment networks with shared access allow the use of repeaters, which are defined for operating speeds up to 1000 Mbps. LAN operation is supported at all speeds. Other specified capabilities include different types of PHY for access networks, PHY suitable for metropolitan network applications, and power supply through selected twisted pair PHY types.

6.1.2.3.9 Cable communication routes

There are several specific communication cable routes in the communication architecture of the technical road facilities. Table 28 Communication cable and wireless routes defines these routes.

Table 29 Communication cable and wireless routes

Route	Purpose	Requirements
Regional telecommunications network for technical facilities	Communication between OT and RCC, between RCC, connection of the RCC and OT to the IT administrator, link to third party IT systems	96-fibre SM optical cable
Regional wireless telecommunications network for technical facilities	Communication between OT and RCC, between RCC, connection of the RCC and OT to the IT administrator, link to third party IT systems alternative route to supplement a redundant connection;	at least 4 to 6G LTE telecommunications operator
control centre computer network	communication between OT components	at least CAT 5e UTP for 1000BASE-T Ethernet LAN according to IEEE 802.3
dedicated VMS network; linking VMS and large-scale displays	video data	type, format, interface and type of cable according to design documentation. Special SM fibres in the optical cable are reserved for VMS and video data
Technical road section telecommunications network	cable connection of control systems	96 or 48-fibre SM optical cable
Road section telecommunications network**	cable connection of control systems	96 or 48-fibre SM optical cable
Technical road section wireless telecommunications network*	wireless interconnection of control systems where a cable route is not available; alternative route to supplement a redundant connection; links to mobile systems; links for cooperative intelligent transport systems	at least 4 to 6G LTE telecommunications operator
Road section wireless telecommunications network**	wireless interconnection of control systems where a cable	at least 4 to 6G LTE telecommunications operator

	route is not available; wireless interconnection of control systems in the case of an off-grid LV power supply system feeding electricity to technical facility distribution frames link to a mobile system; links for cooperative intelligent transport systems	
Process networks – cable connection	cable connections within control systems	UTP or FTP for at least 100BASE-T Ethernet or MM or SM optical cable with a sufficient number of fibres in industrial design or other cable lines given by design documentation
Process networks – wireless connection	wireless connections within control systems, in particular mobile equipment	LAN according to IEEE 802.11
Individual telecommunications interconnections	alternative solution for cable connections and unavailability of telecommunications operators' networks	given by the design documentation

* S1 – level of technical road facilities
** S2 – level of technical road facilities

* and ** networks are LANs according to IEEE 802 standards [ZP6] to [ZP16].

6.1.2.3.10 Allocation of optical cable fibres

According to these TS, allocation of optical cable fibres is given by the design documentation based on a decision of the administrator. In addition, the design documentation shall count on an adequate margin of optical cable fibres. 50 % of free fibres are required for an adequate margin.

6.1.2.3.11 Cable conduits for communication routes

Conduits for communication route cables and the method of their stowage is described in Article 5.1.5 of these TS. Power lines and telecommunications cables shall be laid together in a single space according to the rules laid down in that Article. In the event that telecommunications cables are laid separately, the rules described in Article 5.1 of these TS must be respected. Every situation needs to be addressed in the design documentation.

6.1.2.3.12 Virtual LAN

As mentioned above, the appropriate design and use of virtualisation allows the separation of networks into virtual LANs, VLANs that allow network administrators to logically group network nodes and split networks without the need for major physical infrastructure changes. Technical facility systems of a road section and a technical road section are designed in such a way that they are virtually separated from each other.

6.1.2.3.13 Types of LAN connections

Technical road facilities use two types of LAN HMI connections and controllers: client/server LAN and peer-to-peer LAN. A client/server LAN consists of several devices (clients) connected to A central server. The server manages file storage, application access, device access and network transmission. A client can be any connected device that launches or accesses applications. Clients connect to the server either via cables or via wireless connection. Application files, data and databases are stored on the LAN server. Users and programs access databases, document sharing, print and other services through applications running on the LAN server with read and write access provided by an IT administrator and an OT network administrator. Most technical road facility control system networks are based on client/server LAN networks. A peer-to-peer LAN has no central server and cannot handle

as large workloads as a client/server LAN. In a peer-to-peer network, each controller also participates in the functioning of the network.

6.1.2.3.14 Availability of telecommunications networks

As part of technical road facilities, IT connections are implemented via Ethernet LAN using devices suitable for the indoor environment. OT networks use industrial Ethernet devices. The OT network of a technical road section (level S1 technical and power road facilities) must operate and be available in 24/7 mode. The only exception are special, the administrator approved closures without road traffic. In the event of a malfunction of the OT network, the CRS must stop road traffic and keep it off of the relevant technical road section. In the event of an OT malfunction on a road section (level S2 technical and power road facilities), the operating technical documentation approved by the road administrator is followed.

6.1.2.3.15 Industrial Ethernet

Industrial Ethernet is an application of Ethernet in an industrial environment, as defined in Article 3.4 of these TS, in the outdoor environment, with protocols that provide determinism and real-time control. Cables are connected to equipment by durable connectors and components are used with properties suitable for an industrial environment characterised by extreme temperatures, humidity, aggressive substances and vibrations; for the collection and distribution of signals, data, automation and process control, i.e. process communication within the process and control levels, OT networks are used. Process communication takes place between the control unit and its functional elements.

6.1.2.3.16 Communications interfaces and protocols of process networks

Control unit interfaces and protocols, operating bus specifications and profiles, concept and data types are defined by the series of standards STN EN 61158 and STN EN IEC 61784 Industrial communication networks – specifications and profiles of operational buses. These are networks with communication protocols of different types such as Profibus DP, Modbus RTU, Modbus TCP/IP, Profinet, OPC UA and similar, which meet the conditions of an open industry standard, according to the STN EN 61131 set of standards. The design documentation must always choose a solution that meets the criteria of functionality and cybersecurity. Whenever possible, a technical solution at the physical level should prefer networks based on industrial Ethernet and not serial networks.

If an OpenPLC open source PLC system is used for programming, the requirements of the STN EN 61131 set of standards must be met.

The EN 61131 set of standards covers the use, communication and programming of PLCs and their associated peripherals such as PADT programming and debugging tools, remote devices of RIOS input-output systems, RTU, HMI, control systems and networks. PLCs and their associated peripherals are intended for use in industrial environments and can be provided as open or closed devices. If a PLC or its associated peripherals are intended for use in other environments, then the specific requirements, standards and installation procedures for those other environments must additionally be applied to the PLC and its associated peripherals. The functionality of a programmable driver can also be performed on specific hardware and software platform such as a universal computer or a personal computer with industrial environment characteristics. The STN EN 61131 set of standards applies to all products performing the PLC function and their associated peripherals. PLC, their application program and related peripheral equipment are considered to be components of the control system.

For the sake of security, these technical facility LANs are strictly separated and with strictly controlled access. To interconnect LANs, switches are used or routers to the WAN corresponding to the regional telecommunications network of technical road facilities are used. This connection through networks, including interconnections and Internet accesses, must comply with the prescribed cybersecurity rules, see Article 6.2 of these TS.

Specific communication interfaces and process network protocols are defined in the non-public part of the design documentation.

6.1.3 Data exchange, application protocols and data models

6.1.3.1 Data exchange specifications for traffic control and traffic information.

European standards apply DATEX II according to the following standards for data exchange specifications for traffic management and traffic information:

- background and framework EN 16157-1;
- location reference STN EN 16157-2;
- disclosure of the situation STN EN 16157-3;
- display of signs with variable symbols STN EN 16157-4;
- display of measured and processed data EN 16157-5;
- display of parking STN P CEN/TS 16157-6;
- common data elements EN 16157-7.

DATEX II specifies and defines the components needed to support the exchange and shared use of data and information in the field of transport and travel. Components include the framework and context for the modelling approach, data content, structure data, and relationships. This involves
— traffic and travel information relevant for road networks (municipal and urban);
- information on public transport that is of direct relevance to the use of the road network (e.g. train or ferry services);
— traffic and travel information for Cooperative Intelligent Transport Systems (C-ITS).

In the EU, DATEX II, with the above-mentioned framework set of standards STN EN 16157 , is the international standard for all states. Other alternative formats and data exchange communication protocols for traffic management and traffic information are summarised in Article 6.1.3.2 of these TS.

This article 6.1.3 of these TS does not address the communication interfaces and protocols of the procedural networks dealt with in the relevant sections of Article 6.1.2 of these TS.

When communicating within individual ITS connected via higher-priority control systems, connected higher-level priority systems, it is necessary to collect data and resultant traffic data into files and databases in such a way that the exchange of data for traffic management and traffic information pursuant to this Article 6.1.3 of these TS is made possible in the simplest and most appropriate way. This should involve sharing the contents of files and databases with administrators and third parties as efficiently as possible. All in compliance with the rules of cybersecurity according to Article 6.2 of these TS.

6.1.3.2 Alternative formats and communication protocols for data exchange

In [Z27] and other subsequent Commission Delegated Regulations it is set out that the data collected shall be provided in a simple manner, including remotely, by any relevant means in order to facilitate its remote collection by all operators. Public or private operators and service providers use DATEX II profiles or other internationally compatible formats to ensure the interoperability of information services across the European Union. For the purpose of sharing and exchanging data, the DATEX II format or any international machine-readable format compatible with DATEX II is used.

[L5] lists DATEX II as the recommended required standard and specification for the above interfaces. Since it is an EU implementation document, the recommended DATEX II standard is considered the most appropriate.

This Article 6.1.3.2 of these TS sets out alternative formats and communication protocols for data exchange for traffic management and traffic information for Article 6.1.3.1 of these TS. This set is not exhaustive and there are other options. The data exchange specifications for traffic management and traffic information follows the design documentation approved by the administrator. The application of

communication protocols must comply with the rules of cybersecurity pursuant to Article 6.2 of these TS.

6.1.3.3 Data exchange entities and types of information content

Data exchange specifications are used between two of the following entities:

— Traffic Information Centres (TICs);

— Traffic Control Centres (TCCs);

— Service Providers (SP).

for at least the following types of information content:
- information on road traffic events;
- planned and unscheduled events on the road network and in the surrounding environment;
- information on activities initiated by the operator, including advisory and mandatory measures;
- road traffic measurement data, status data and travel time data;
- travel information relevant for road users, including weather and environmental information;
- traffic control information and information and advice on the use of the road network.

This approach is described using formal methods and provides a reference framework given by the STN EN 16157 set of standards.

6.1.3.4 Data exchange with C-ITS systems and third parties

The intelligent transport system, as well as public communications networks, mediate and, in some cases, directly provide the communication of specific data to higher-priority control systems of the road administrator and to level 3 or 4 higher-priority systems, police, rescue services and other entities. These are specific e-Call, C-ITS, CCAM, C-ITS in urbanised environments, and C-ITS in border and cross-border areas, traffic infractions and strict liability, vehicle navigation systems, vehicle infotainment systems, travel information systems, electromobility and renewables, MaaS, urban air mobility, etc., some of which are in place and fully operational, and some are being developed and can be expected to play an increasingly important role from the point of view of the professional, the public and carriers. This is data and information based on big data, which allows the administrator to obtain and request additional significant and useful functionalities from the system.

For more detailed general requirements for systems referred to in this article, their interconnection and data exchange, see Article 4.5.14 of these TS.

6.1.3.5 Objectives in relation to data exchange

The objectives of the above requirements are:
- promoting traffic safety;
- facilitating the achievement of the LoS service level, i.e. traffic flow;
- innovation-supported re-regulation and governance;
- contribution to environmental and climate sustainability.

6.2 Cybersecurity

6.2.1 Cybersecurity legislative framework

The basic legislative framework for cybersecurity issues consisting of the provisions of the Act [Z16] and its implementing legislation. This means that the requirements for compliance with general security measures must be met at least to the extent of the security measures pursuant to [Z16] § 20, in accordance with the provisions of the Act [Z20] and its implementing legislation, in particular the Decree [Z19] of the National Security Authority, which lays down the content of security measures, the content and structure of the safety documentation and the scope of general security measures. Another framework consists of related technical standards (STN EN ISO/IEC) together with departmental technical regulations for the road transport sector. The security measures proposed shall be consistent with and correspond to the security strategy and security policies of administrators (‘security documentation’) and the TPR. According to the above, the technical solution, design, implementation and operation of equipment, technical and power facilities, including ITS on roads,

must be in compliance. When applying the provisions of individual acts, standards and regulations, it is necessary to take into account the nature of the objects addressed and the proposal must be discussed and agreed with the Customer, which in case of implementation represents the interests of the administrator. The method of categorisation and content of public administration information technology security measures is stipulated pursuant to [Z38].

6.2.2 Technical normative framework for cybersecurity

The ISO/IEC 27019 and STN EN IEC 62443-2-4 standards shall be used as follows: ISO/IEC 27019 is a guide based on ISO/IEC 27002 applied to process control systems used in the energy services sector to control and monitor the generation or generation, transmission, storage and distribution of electricity, gas, oil and heat and to control related support processes, including in particular central and distributed process control, monitoring and automation technology, and information systems used for their operation, such as programming and parametrisation equipment. It also includes digital controllers for automation components such as control and operation devices or PLCs, including digital sensor elements and actuators. It also includes all other supporting information systems used in the field of process management, data visualisation tasks and for control, monitoring, data archiving, history recording, reporting and documentation purposes; communication technologies used in process control, e.g. network, telemetry, remote control applications and remote control technology; Advanced Metering Infrastructure (AMI) components – smart meters; instruments for measuring emissions; digital protection and security systems; protective relays, safety PLCs, emergency control mechanisms; energy management systems, distributed energy resources (DER), electricity charging infrastructure in private residential buildings or customers' industrial facilities; distributed components of smart grid environments; all software, firmware and applications installed on the above systems; any premises in which the above facilities and systems are located; remote maintenance systems for these systems. The main principles based on ISO/IEC 27002 are represented by the 'Code of Procedures for Information Security Controls' for information security management applied to process management systems. ISO/IEC 27002 is applied to the field of process control systems and automation technology, which implements a standardised and specific information security management system (ISMS) in accordance with ISO/IEC 27001 up to the process management level. In addition to safety objectives and measures under ISO/IEC 27002, these include special specific requirements for the development, operation, repair, maintenance and operating environment of process control systems. Process technology is an integral part of critical infrastructure as it is essential for the safe and reliable operation of infrastructures. Differences and characteristics must be duly taken into account in the control processes for process control systems and justify separate application within the ISO/IEC 27000 set of standards.

In terms of design and function, process control systems are information processing systems. They collect process data and monitor the state of physical processes using sensors. The systems process this data and generate control outputs that regulate activities through actuators. Control and regulation is automatic, but manual operator intervention is also possible. Information and information processing systems are therefore an essential part of the operational processes within the services. It is important that appropriate safeguards are applied in the same way as in the case of other organisational units. Software and hardware components and programmable logic based on standard ICT technology must be used in process management environments. The risks arising from the trend of increasing system complexity must be evaluated during risk assessment. Information and information processing systems in process management environments are also exposed to an increasing number of threats and vulnerabilities. Appropriate information security must be achieved in process management through the implementation and continuous improvement of ISMS in accordance with ISO/IEC 27001. Effective information security in process management shall be achieved by establishing, implementing, monitoring, reviewing and, where necessary, improving applicable measures in order to achieve the organisation's specific security and business objectives. Particular attention must be paid to the specific role of administrators in the company and to the economic necessity of secure and reliable energy supply and operation of infrastructure. The overall success of cybersecurity of energy relevant industries and infrastructure is based on joint efforts by all stakeholders.

ISO/IEC 27000 series standards represent international standards in the field of information security management derived from the British standards of the BS 7799 series. The overview kept by CSIRT MIRRI SR [Computer Incident Response Team of the Ministry of Investment, Regional Development and Informatics of the Slovak Republic] contains the names and designations of the individual standards together with their description.

STN EN IEC 62443-2-4 specifies a comprehensive set of security feature requirements for IACS service providers that they can offer to the owner and administrator during the integration and maintenance of the automation solution. Because not all requirements apply to all industry groups and organisations, the standard provides the development of profiles that allow a subset of these requirements. Profiles are used to adapt this document to specific environments, including non-IACS based environments. The STN EN IEC 62443 set of standards is suitable for addressing the cybersecurity of industrial OT systems and includes the following areas:

STN EN IEC 62443-1 General terminology, policies, cybersecurity models;

STN EN IEC 62443-2 Process management, organisational cybersecurity assurance and operator requirements;

STN EN IEC 62443-3 recommendations and requirements from the point of view of systems, requirements for integrator, contractor, of which specifically
- STN EN IEC 62443-3-1 security technologies for OT;
- STN EN IEC 62443-3-2 risk management in the design of systems;
- STN EN IEC 62443-3-3 system safety requirements and security levels;

STN EN IEC 62443-4 recommendations and requirements from the point of view of instruments, terminal equipment, manufacturer's requirements.

6.2.3 CSIRT and CERT Cybersecurity Recommendation Framework for IT and OT

The principles of IT and OT cybersecurity, all parts of the ICT of road equipment, technical and power facilities must follow the basic recommendations for all essential service operators operating industrial facilities. 'CERT' is a registered trademark. The national SK-CERT unit is a certificate holder.

The NSA cooperates with central authorities, other government authorities and CSIRT units, operators of essential services and digital service providers in the performance of tasks under the Cybersecurity Act. The NSA accredits the CSIRTs, except the National CSIRT and the Government CSIRT, and places them on the list of accredited CSIRTs. The Authority establishes the National Cybersecurity Centre as its organisational unit, which has the status of a national CSIRT with competence for the Slovak Republic. The National SK-CERT is awarded the highest degree of membership as a Trusted Introducer – 'Certified' status, which makes it one of the most advanced CSIRTs/CERTs.

The organisation communicates with CSIRTs and SK-CERTs through the Cybersecurity Manager at least:
- due to the reporting of a critical security incident; and
- to seek help and recommendations in dealing with security incidents.

6.2.4 Recommendations for IT and OT cybersecurity

According to SK-CERT, OT systems (also referred to as ICS – Industrial Control System or IACS – Industrial Automation and Control Systems) are used to signal and monitor, measure and regulate, manage and control industrial technical facilities from various areas and sectors such as manufacturing, chemical, gas, metallurgical, energy, transport, water management and others.

OT system terminals are various instruments (hardware including software) with specific functions such as, in our case (for the purposes of these TS), in particular, PLC, PC, DCS, SCADA components and units, remote control terminals, automated building systems, control systems for road sections and technical road sections. A cyber-attack against the OT system is not only a threat of damage to the terminal equipment itself, but above all a threat of damage of a significantly larger scale to the technology itself, road equipment, technical and power facility systems, with a potential impact on people's lives, health and property, as well as a potential threat to the environment. Cybersecurity of IT and OT systems is a similar topic in its basic features. Nevertheless, OT systems have their own specifics. A comparison of the characteristic characteristics of the systems is shown by the following Table 30 with modified and supplemented characteristics specifically for the transport sector, namely the technical road facilities.

Table 31 Comparison of specifics of IT and OT systems

ICT systems	IT	OT (ICS, IACS)
Main processes	processing of information	management of technological processes
Life cycle	4-6 years	15-20 years
Patch management	2 to 3x per year	1x per year to 1x in 2 years
Availability	outages accepted	24/7
Communication protocols	TCP/IP	IEC, EN IEC and STN EN IEC 61850, 61131, 16157

6.2.5 Ensuring a high common level of cybersecurity

The European Economic and Social Committee (EESC) calls for an active EU cyber defence policy and stresses the need for better preparation for cyber-attacks targeting in particular critical infrastructure. [Z34] recommends that EU Member States commit to a continuous rapid response and evaluate the cyber preparedness and performance of EU cyber crisis response mechanisms, also focusing on critical sectors identified in the Directive [Z33].

Reducing the EU's dependence on third countries is essential to ensure the EU's strategic autonomy. The EESC considers it essential for the EU to adopt a medium-term approach to autonomy in key technologies and calls for research and production facilities set up by EU-based companies and that the relevant European industrial policy should focus on: autonomous Cybersecurity Ecosystem. In order to support the EU's cybersecurity autonomy, it is necessary to establish a dynamic real-time testing and information exchange platform or take it over from the private sector, focusing on identifying capabilities currently lacking. In [Z33] and the Critical Entities Resilience Directive, specific national and sectoral obligations for the EU cyber defence framework are in place. Investments in cyber defence must be prioritised to protect EU citizens and critical infrastructure. IoT devices must be protected as well as traditional devices and the EESC calls for a minimum level of security to be ensured through IDAM platforms. Certification is a key method to ensure a higher level of security, and the new EU approach to certification places greater emphasis on securing the Internet of Things. Public-private partnerships have proven to be the most effective approach to improving the cybersecurity of the entire digital ecosystem, but they cannot be one-way as public institutions need to share their information with the private sector.

Pursuant to [Z33], given the rapidly evolving threat landscape, resilience measures should be taken as a matter of priority in key sectors such as: energy, digital infrastructure, transport and space, as well as in other relevant sectors identified by Member States. Such measures should aim at increasing the resilience of critical infrastructure, taking into account relevant risks, in particular cascading effects, supply chain disruption, dependency, impacts of climate change, unreliable vendors and partners, and hybrid threats and campaigns, including manipulation and interference of foreign information. With regard to national critical infrastructure, given the possible consequences, priority must be given to critical infrastructure with significant cross-border validity. Member States are invited to swiftly implement such resilience measures, while maintaining the approach set out in the legal framework.

Energy and transport sectors are affected by threats related to digital infrastructure in the context of equipment containing digital components. The security of related supply chains is important for the continuity of the provision of essential services and for the strategic control of critical infrastructure in the energy sector. These circumstances must be taken into account by the administrator when taking measures to increase the resilience of critical infrastructure in accordance with this Recommendation. It must be ensured that Member States and their infrastructure managers achieve implementing the measures recommended in the EU's 5G Cybersecurity Toolbox and defining restrictions for high-risk suppliers given that delays may increase the vulnerability of networks in the state and in the EU. Physical and non-physical protection of critical and sensitive parts of 5G networks must be strengthened, including through strict access controls. In addition, the need for complementary measures to ensure a consistent level of security and resilience of 5G networks needs to be assessed.

6.2.6 Principles of cybersecurity architecture

The basic principles of the cybersecurity architecture according to SK-CERT are:

- Security by design, cybersecurity features must be an essential part of component design and development;
- Minimal need-to-know principle, cybersecurity features must be user-friendly and must not require admin-level knowledge;
- Defence-in-depth principle, the principle of complex cybersecurity solutions on multiple levels;
- Redundancy principle, the basic principle of operational security that ensures that an individual failure does not render the whole or a significant part of the system inoperable and unavailable.

The MAIN principles of information security are:
- ensuring the confidentiality of transmitted data;
- ensuring the integrity and integrity of transmitted data throughout the transmission path;
- ensuring the availability of transmitted data.

6.2.7 Principle of dealing with the lifecycle of an information asset and a security incident

Types of measures in the context of the information asset's life cycle [L11]:
- existing measures are inherently embedded already at the time of design or implementation of the system;
- extended (improved) measures are applied to the implemented system in order to treat a risk already identified in the normal operation of the system; they are typically proposed by a member of staff responsible for coordinating cybersecurity and information security;
- additional measures are recommended by the auditory in the audit report to address the risk identified in the cybersecurity audit.

For the implementation of risk reduction measures, measures need to be divided into:
- operational, the implementation of which is not demanding from a time and financial point of view, but has an immediate effect on risk reduction;
- systemic, organisational and broader technical measures with a long-term risk reduction effect.

The sequence in which the proposed measures will be implemented, the so-called implementation plan, is elaborated within the framework of a security strategy or a security project. This programme depends on a number of factors that need to be taken into account in its design. Such factors include:
- priorities resulting from the risk assessment;
- the expenditures necessary to implement the measures;
- readiness and capability of the organisation to implement measures (technical, organisational, financial);
- support by the organisation's management for implementation of the measures.

In the process of dealing with a cyber security incident and a serious cyber security incident, the following activities take place:
- identification of the nature of the reported cybersecurity incident (security incident classification);
- identifying the extent of a cyber security incident (organisational entities and systems concerned);
- establishing a priority for the resolution of the cybersecurity incident and key objectives such as:
    - complete or partial correction;
    - restoration of the original state;
    - identification of the origin of the cyber security incident;
    - limiting the spread of a cyber security incident;
    - elimination of the cause of a cyber security incident, etc.;
- a preliminary estimate of the difficulty of dealing with the cyber security incident;
- the decision to inform employees of the organisation or, where appropriate, other affected organisations/persons, government institutions or the public;
- stipulating the solution and the necessary capacities;
- identification of the relevant qualification skills needed to resolve the cyber security incident;
- a decision on the possible involvement of external actors in the handling of the cyber security incident;
- a decision on the possible legal continuation of incident resolution;
- managing the resolution of the cyber security incident according to a defined procedure;
- while addressing the cyber security incident, correcting estimates, decisions and established procedure, as appropriate;
- deciding on how to close the incident;
- deciding on corrective measures.

6.2.7.1 Cybersecurity audit

The administrator must perform a cybersecurity audit based on [L11].

6.2.7.2 Testing specific properties from a cybersecurity perspective

Article 6.2.7.1 of these TS contains a requirement to carry out a cybersecurity audit. However, when work is being delivered, this does not have to involve a complete cybersecurity audit, but rather testing specific properties from the perspective of the cybersecurity of the work being delivered.

6.2.8 Minimum technical requirements for OT cybersecurity

Minimum technical requirements for cybersecurity of OT systems, the concept of 'defence-in-depth' requires that the minimum technical requirements for cybersecurity at the level of the individual components apply to each individual OT device – terminal equipment (containing elements such as a microprocessor unit, operating system and communication interfaces). Individual functions of active cyber security defence-in-depth must be implemented at the level of the hardware and operating system of terminal equipment.

The specific minimum technical requirements depend on the specific applications of the individual systems in which the apparatus is used. The availability of the OT system of road equipment, technical and power facilities, which is supposed to be 24/7 for a technical road section, applies to those parts of the technical facilities that are identified in the design documentation for implementation and the operational documentation approved by the administrator, and these parts meet the appropriate minimum technical requirements for cybersecurity. Similarly as stated in Article 2.3.1 for redundancy, the level of cybersecurity must be properly designed so that it does not result in less rather than more reliability and availability of systems – in order not to create an overly complex system that is prone to various problems and malfunctions.

The design and operating documentation must also include solutions for the cyber-attack detection system and the cyber-attack prevention system at the level stipulated by legislation. These solutions, together with this documentation, must be approved by the road administrator. In addition to spare parts for OT, there must also be provisions for upgrade and support (patch management) by the manufacturer for the entire life of the system (at least 15 to 20 years). The operating documentation must also include procedures for dealing with OT cyber incidents.

Minimum technical requirements to ensure cybersecurity shall be applied pursuant to [T22] for all technical road facility control systems appropriately as indicated in the approved design documentation. These minimum technical requirements are stipulated according to the categorisation of the criticality of systems within the meaning of [Z16] and [Z19].

6.3 Summary of common requirements for telecommunications network and cybersecurity

6.3.1 Road telecommunications network. Common requirements – summary

6.3.1.1 In general

Road telecommunications networks provide data transmission within a road's equipment, technical and power facilities. Data transmissions perform communication between OT systems, control units, between various systems, between certain devices, communication within process networks, transmission to control systems and to higher-priority control systems, or their mutual communication, transfers for the needs of IT administrators, the ability to connect to the administrator’s contractual partners, interconnection with C-ITS, transmissions for IT systems of the police, fire and rescue, systems with higher priority 3 or 4, intelligent transport systems, MaaS, interconnection to international intelligent transport systems, mobility and MaaS systems, and interconnections to the it systems of road administrators of various infrastructural and transport importance.

6.3.1.2 Design

See Chapter 8 of these TS.

6.3.1.3 Implementation

The implementation of a road telecommunications network is based on legislation, technical standards, TPR and the rules set out in Article 6.1 of these TS.

6.3.1.4 Operation and maintenance

The operation and maintenance of a road telecommunications network is based on legislation, technical standards, TPR and the rules set out in Article 6.1 of these TS.

6.3.2 Cybersecurity. Common requirements – summary

6.3.2.1 In general

Compliance with the rules and procedures for the implementation of cybersecurity processes should ensure cybersecurity of data, information and systems of technical road facilities, the road telecommunications network, and road power supply infrastructure control systems.

6.3.2.2 Design

Basics assumptions – see Chapter 8 of these TS.
Cybersecurity must comply with the requirements set out in Article 6.2 of these TS.

6.3.2.3 Implementation

In the implementation of cybersecurity, it is necessary to comply with the requirements set out in Article 6.2 of these TS.

6.3.2.4 Operation and maintenance

During operation and maintenance, it is necessary to comply with the requirements set out in Article 6.2 of these TS.

7 Operation and maintenance

Chapters 4, 5 and 6 contain summary common operational and maintenance requirements for each area covered by the chapters, always in the relevant article at the end of the chapter and, where appropriate, in some other articles. Items for maintenance, technical inspections, repairs and lists of spare parts, instructions for use and building operating manuals are recorded in the BIM system as specified in Article 2.2.2.2.4.

In addition, commissioning and carrying out technical inspections are important for operation and maintenance. The requirements for the relevant actions are set out in [T19].

8 Design and documentation

8.1 General requirements for design documentation for technical facilities

The design and creation of design documentation for an information technology system (i.e. equipment, technical and power facilities including ITS systems on roads) is governed by [T5].

The construction project addresses documentation of objects, the list of which is given in Article 4.6 of these TS. Step-by-step development and details are presented in the individual stages of the project documentation. The documentation is divided into a building and technology part.

The construction project must comply with the requirements of [Z9] and [Z23].

8.2 General principles for project preparation for technical facilities

The basic basis for design documentation for equipment, technical and power facilities is the road design documentation prepared according to the mandatory legislative framework [Z9] and [Z23] STN 73 6100 ST N 73 6101, other STN, TPR and road administrator requirements.

In terms of composition and structure, the design documentation for equipment, technical and power facilities is divided into objects by system. The actual distribution and implementation of the requirements is carried out according to the above procedures.

Each design documentation for technical facilities must contain: identification of higher-priority systems pursuant to Article 4.4.2 of these TS.

Explanation and justification of classification classes, environment, impacts and levels of technical road facilities pursuant to Chapter 3 of these TS.

The consistency of the design with [Z8], [Z9] and [Z43] shall be explained and justified.

In each type (stage) of documentation, lines, symbols and markings shall be used pursuant to [T5], [T22] and Article 2.2.2.2.4 of these TS.

The implementation of BIM is specified in Article 2.2.2.2.4 of these TS.

All other design and documentation requirements are listed in [T5].

8.3 As-built documentation

Pursuant to [T5], for each construction of a road, its modernisation, reconstruction, or its modification, as-built documentation must be prepared. Obtaining as-built documentation is the responsibility of the Contracting Authority, through the Contractor. After completion and acceptance of the Work, or after approval, the Contracting Authority will hand over the as-built documentation to the relevant property manager of the road, or the given building, who will keep this documentation for the entire life of the structure.

Details of the content and scope of as-built documentation are set out in [T5].

9 Life cycle of technical road facilities

9.1 Life cycle

The life cycle of equipment, technical and power facilities including intelligent transport systems on a road requires regular inspections, maintenance and repairs [T19]. Table 15 these TS assume the life of OT systems to be 15 to 20 years and the life of IT systems to be 4 to 6 years. The design life of technical facilities and safety gear (equipment) is shown in Table 3 of [T19]. From an analysis of past inspections, which should also include assessments of the functionality of the systems, it is possible to propose the scope and time requirements for their upgrade.

9.2 Recycling and disposal

Used end-of-life components and non-repairable parts of road equipment, technical and power facilities require recycling and disposal in accordance with applicable legislation. The life of technological and safety equipment and the life cycle of components and systems is addressed by [T19] as a series of stages through which an object passes from its conception to disposal.