



Minimum requirements for an authorisation to remotely drive automated vehicles in Switzerland

**Mindestanforderungen für eine Genehmigung der
Fernlenkung von automatisierten Fahrzeugen in der Schweiz**

**Exigences minimales pour une autorisation de conduire à
distance des véhicules automatisés en Suisse**

HEIA-FR (ROSAS)

Roland Scherwey
Gabriel Python
Gabrielle Thurnherr
Denis Rosset

BFH

Raphael Murri
Peter Affolter
Ahmed Hanachi
Arne Keller

DTC Dynamic Test Center AG

Reto Röthlisberger
Alphonse Frésard

CertX SA

Vincent Sabot
Loan Bétend

Eraneos Switzerland AG

Fabian Zumkehr

LOXO AG

Amin Amini
Claudio Panizza

Der Inhalt dieses Berichtes verpflichtet nur den (die) vom Bundesamt für Strassen unterstützten Autor(en). Dies gilt nicht für das Formular 3 "Projektabschluss", welches die Meinung der Begleitkommission darstellt und deshalb nur diese verpflichtet. Bezug: Schweizerischer Verband der Strassen- und Verkehrsfachleute (VSS)

Le contenu de ce rapport n'engage que les auteurs ayant obtenu l'appui de l'Office fédéral des routes. Cela ne s'applique pas au formulaire 3 « Clôture du projet », qui représente l'avis de la commission de suivi et qui n'engage que cette dernière. Diffusion: Association suisse des professionnels de la route et des transports (VSS)

La responsabilità per il contenuto di questo rapporto spetta unicamente agli autori sostenuti dall'Ufficio federale delle strade. Tale indicazione non si applica al modulo 3 "conclusione del progetto", che esprime l'opinione della commissione d'accompagnamento e di cui risponde solo quest'ultima. Ordinazione: Associazione svizzera dei professionisti della strada e dei trasporti (VSS)

The content of this report engages only the author(s) supported by the Federal Roads Office. This does not apply to Form 3 'Project Conclusion' which presents the view of the monitoring committee. Distribution: Swiss Association of Road and Transportation Experts (VSS)

Minimum requirements for an authorisation to remotely drive automated vehicles in Switzerland

Mindestanforderungen für eine Genehmigung der Fernlenkung von automatisierten Fahrzeugen in der Schweiz

Exigences minimales pour une autorisation de conduire à distance des véhicules automatisés en Suisse

HEIA-FR (ROSAS)

Roland Scherwey
Gabriel Python
Gabrielle Thurnherr
Denis Rosset

BFH

Raphael Murri
Peter Affolter
Ahmed Hanachi
Arne Keller

DTC Dynamic Test Center AG

Reto Röthlisberger
Alphonse Frésard

CertX SA

Vincent Sabot
Loan Bétend

Eraneos Switzerland AG

Fabian Zumkehr

LOXO AG

Amin Amini
Claudio Panizza

**Research project MB4_20_02E_01 at the request of Mobility 4.0 (MB4)
January 2025 | 1791**

Imprint

Research centre and project team

Project management

Roland Scherwey

Raphael Murri

Members

Ahmed Hanachi

Alphonse Frésard

Amin Amini

Arne Keller

Claudio Panizza

Denis Rosset

Fabian Zumkehr

Gabriel Python

Gabrielle Thurnherr

Loan Bétend

Peter Affolter

Reto Röthlisberger

Vincent Sabot

Advisory commission

President

Martin Neubauer

Members

Benno Nager

Bernhard Riegel

Bettina Zahnd

Jesper Engdahl

Rico Schwendener

Sylvain Pasini

Thomas Probst

Applicant

Bundesamt für Strassen (ASTRA), Forschungsbereich ASTRA

Source

The document can be downloaded free of charge from

<https://www.mobilityplatform.ch>

Table of Contents

List of Illustrations	8
List of tables.....	10
List of Abbreviations.....	11
Zusammenfassung.....	14
Résumé	28
Summary	42
1 Introduction	56
1.1 Context and Current Situation	56
1.2 Motivation and Objectives of the Research Project.....	60
1.3 Report Structure and How to Read the Report	62
1.4 What Is Not Covered	63
2 Fundamental Information.....	64
2.1 Introduction	64
2.2 International and National Research	64
2.2.1 Introduction.....	64
2.2.2 International Projects and Papers	64
2.2.3 National Projects and Papers.....	72
2.2.4 Summary	74
2.3 Legal Frameworks	75
2.3.1 Overview	75
2.3.2 European Union	76
2.3.3 International Harmonization Efforts	76
2.4 Legal Acts.....	77
2.4.1 Overview	77
2.4.2 International Legal Acts	77
2.4.3 National Legal Acts.....	80
2.4.4 Summary	84
2.5 Standards.....	85
2.5.1 Overview	85
2.5.2 International Standards (ISO).....	85
2.5.3 Harmonized European Standards	87
2.5.4 National Guidelines	87
2.5.5 Summary	88
2.6 The Role of Standards in Public Procurement	89
2.7 Overview of Remote Operation Station Providers	90
2.7.1 Summary	93
2.8 Insights from Operators in Switzerland	94
2.8.1 Feedback From an On-Board Operator of an AV for Public Transport.....	94
2.8.2 Survey Results from LOXO Operators.....	95

2.8.3 Summary.....	96
3 Methodology	97
3.1 Research Methodology.....	97
3.2 Research Plan.....	99
4 Results.....	101
4.1 Terminology.....	101
4.1.1 Introduction	101
4.1.2 Definitions.....	101
4.1.3 Minimum Risk Manoeuvre (MRM)	105
4.1.4 Use Cases and Applications	106
4.2 Remote Operation Level (ROL)	109
4.2.1 Overview.....	109
4.2.2 Taxonomy of Driving Automation According ISO/SAE PAS 22736	109
4.2.3 Taxonomy of Teleoperated Driving.....	109
4.2.4 Taxonomy for Remote Operation	110
4.3 Scenarios	115
4.3.1 Introduction	115
4.3.2 Use Cases.....	115
4.3.3 Identification and description of relevant Scenarios	117
4.3.4 Selected Scenarios.....	117
4.4 Definition of Requirements	128
4.4.1 Overview.....	128
4.4.2 Requirement Definition	128
4.4.3 Requirement Categories.....	132
4.4.4 Elaboration of the Requirements	133
4.4.5 Cybersecurity Requirements.....	136
4.4.6 Summary.....	138
4.5 Requirements Validation	139
4.5.1 Introduction	139
4.5.2 Scenarios and List of Requirements	139
4.5.3 Validation Methods.....	140
4.5.4 Application and Results	142
4.5.5 Validation of Performance Values with Theoretical and Experimental Methods for the Latency Requirements	147
4.5.6 Cybersecurity.....	152
4.5.7 Summary.....	153
4.6 Testing on Site.....	154
4.6.1 On-Site Test Concept and Instrumentation	155
4.6.2 On-Site Test Results.....	165
4.6.3 Discussion and Conclusion	173
4.7 Cybersecurity Tests	174
4.7.1 Introduction	174
4.7.2 Penetration testing approach.....	174

4.7.3	System Under Consideration.....	174
4.7.4	Methodology.....	175
4.7.5	Attack Paths.....	175
4.7.6	Cybersecurity Test Results.....	176
4.7.7	Discussion and Conclusion.....	181
5	Identified Future Research Needs.....	182
5.1	Introduction	182
5.2	Identification of Research Gaps	182
5.3	Technical Report of the Working Group BAST	184
5.4	Recommendations and Prerequisites.....	187
5.4.1	Focus on Safety as a fundamental principle	187
5.4.2	Refinement and Expansion of Scenario Definitions	187
5.4.3	Technological Development and Adaptation to New Standards.....	188
5.4.4	Refinements for Teleoperation (ROL2).....	189
5.4.5	Periodic Review and Further Development.....	190
5.4.6	Training and Certification for Remote Operators 190	
5.4.7	Alignment with International Standards.....	190
5.4.8	Summary	193
6	Conclusion.....	194
7	Appendix	196
7.1	A1 - List of Minimum Requirements	197
7.1.1	Requirements Remote Operation Level (ROL)	197
7.1.2	Requirements Scenarios-Based	201
7.1.3	Cybersecurity Requirements	210
7.2	A2 - Levels of Driving Automation According to ISO/SAE PAS 22736:2021.....	243
7.3	A3 - Taxonomy of Remote Operation Levels (ROL)..	245
7.4	A4 – Details Cybersecurity Test Results.....	246
7.4.1	Remote Operator Station.....	246
7.4.2	Remote Vehicle	253
7.4.3	Communication	254
7.4.4	Remote Operator	255
7.5	A5 - Survey Results from LOXO Operators	256
	Bibliography	260
	Project Conclusion.....	267

List of Illustrations

Figure 1: National projects for public transportation.....	57
Figure 2: National projects for goods delivery and agricultural automation	57
Figure 3: Overview of Remote Operation Systems.....	59
Figure 4: Transition towards automated mobility	60
Figure 5: Report structure	62
Figure 6: Categories of remote-control challenges.....	65
Figure 7: User requirements for remote Teleoperation-based interfaces	66
Figure 8: Summary of the findings regarding human performance	67
Figure 9: DriveU.auto autonomous vehicle Teleoperation Taxonomy	68
Figure 10: Cruise's system verification process.....	69
Figure 11: Stopping distance in case of remote latency	70
Figure 12: Process chain for designing a HMI for a Remote Operator Station	71
Figure 13: SwissMoves proof of concept for Teleoperation of AV.....	72
Figure 14: LOXO Alpha automated delivery vehicle	72
Figure 15: Swisscom's monitoring solution.....	73
Figure 16: Overview of regulations, standards and guidelines.....	76
Figure 17: UNECE WP.29 organization with its 6 working parties.....	79
Figure 18: Overview of the ISO 26262 series of standards	86
Figure 19: Project overview with work packages.....	99
Figure 20: LOXO's Remote Operation Centre	100
Figure 21: Dynamic Test Centre's test track.....	100
Figure 22: Remote Operation System with tasks and roles	101
Figure 23: Sample Use Case sequence DDT.....	102
Figure 24: ROL1 - Representation of Direct Control without OEDR sensors	111
Figure 25: ROL2 - Representation of Direct Control with OEDR sensors	112
Figure 26: ROL3-4 - Representation of Indirect Control.....	113
Figure 27: Taxonomy of Remote Operation Levels (ROLs)	114
Figure 28: Automated Delivery on last mile Use Case (LOXO)	116
Figure 29: Last mile passenger transportation by automated shuttle Use Case	116
Figure 30: Automated bus depot Use Case (SwissMoves AutoDepot project).....	116
Figure 31: Overview of selected scenarios.....	118
Figure 32: Scenario 1 - Representation of unexpected road blockage	119
Figure 33: Scenario 1 - Unexpected road blockage resolution using ROL4	119
Figure 34: Scenario 1 - Unexpected road blockage resolution using ROL3	119
Figure 35: Scenario 1 - Unexpected road blockage resolution using ROL2	119
Figure 36: Scenario 2 - Representation of loss of network	120
Figure 37: Scenario 2 - Loss of network resolution using ROL1	120
Figure 38: Scenario 3 - Representation of imprecise location	121
Figure 39: Scenario 3 - Imprecise location resolution using ROL2	121
Figure 40: Scenario 4 - Representation of solar radiation	122
Figure 41: Scenario 4 - Solar radiation resolution using ROL2	122
Figure 42: Scenario 4 - Solar radiation resolution using ROL1	122
Figure 43: Scenario 5 - Representation of ambiguous sensor results	123
Figure 44: Scenario 5 - Ambiguous sensor results resolution using ROL4.....	123

Figure 45: Scenario 5 - Ambiguous sensor results resolution using ROL3	123
Figure 46: Scenario 6 – Representation of adverse weather conditions	124
Figure 47: Scenario 6 - Adverse weather conditions resolution using ROL3	124
Figure 48: Scenario 6 - Adverse weather conditions resolution using ROL2	124
Figure 49: Scenario 6 - Adverse weather conditions resolution using ROL1	124
Figure 50: Scenario 7 – Representation of bottleneck in dense traffic.....	125
Figure 51: Scenario 7 - Bottleneck in dense traffic resolution using ROL4	125
Figure 52: Scenario 7 - Bottleneck in dense traffic resolution using ROL3.....	125
Figure 53: Scenario 7 - Bottleneck in dense traffic resolution using ROL2.....	125
Figure 54: Scenario 7 - Bottleneck in dense traffic resolution using ROL1	126
Figure 55: Scenario 8 - Representation of false positive obstacle detection.....	127
Figure 56: Scenario 8 - False positive obstacle detection resolution using ROL4.....	127
Figure 57: Scenario 8 - False positive obstacle detection resolution using ROL3.....	127
Figure 58: Scenario 8 - False positive obstacle detection resolution using ROL2.....	127
Figure 59: Form of requirements.....	129
Figure 60: Derivation of the minimum requirements	132
Figure 61: Overview of identified minimum requirements	134
Figure 62: Cybersecurity-relevant elements of the Remote Operation System.....	137
Figure 63: Definition of latencies	147
Figure 64: Braking distance vs. speed with and without latency.....	150
Figure 65: Highest possible speed v_t of the teleoperated vehicle.....	151
Figure 66: Highest acceptable latency t_l of the teleoperated vehicle	151
Figure 67: Test set-up LOXO Alpha and BFH Smartshuttle	155
Figure 68: Aerial view, DTC test drive area, slalom and parking testing tracks.....	156
Figure 69: Aerial view of the slalom course	156
Figure 70: Setup for the parking tests	157
Figure 71: Parking test procedure	157
Figure 72: Setup for scenario test with “false positive”-obstacle in place.....	158
Figure 73: LOXO Alpha automated vehicle for last mile delivery	159
Figure 74: LOXO Remote Operation Centre in Fribourg	160
Figure 75: BFH Smartshuttle automated vehicle for people transportation.....	161
Figure 76: BFH Remote Operation Centre in Vauffelin.....	162
Figure 77: Measurement equipment on LOXO Alpha	163
Figure 78: Antenna and camera positioning on LOXO Alpha	163
Figure 79: Network used for the tests on site at DTC	164
Figure 80: Location data of the BFH Smartshuttle slalom tests	165
Figure 81: Location data of the LOXO slalom tests.	166
Figure 82: Mean distance from mean run for both vehicles.....	166
Figure 83: Parking tests BFH Smartshuttle.....	167
Figure 84: Parking tests LOXO Alpha	167
Figure 85: Scenario 8 - "Bypassing" solution	171
Figure 86: Scenario 8 - "Running over" solution.....	172
Figure 87: Teleoperation diagram from BASt Report.....	184

List of tables

Table 1: Challenges overview.....	74
Table 2: Most relevant articles from OCA/VAF Chapter 5: Driverless vehicles.....	83
Table 3: Legal frameworks overview	84
Table 4: List of Remote Operation Station providers	92
Table 5: Challenges faced by Remote Operation Station providers	93
Table 6: Overview of the experiences of operators in Switzerland.....	96
Table 7: Mobility Use Cases.....	106
Table 8: Agriculture Use Cases.....	107
Table 9: Airport Use Cases	107
Table 10: Mining Use Cases.....	108
Table 11: Logistic Use Cases	108
Table 12 : List of selected scenarios.....	118
Table 13: Description of requirement definitions	131
Table 14: Remote Operator requirements (examples)	134
Table 15: Remote Vehicle Requirements (examples).....	135
Table 16: Communication requirements (examples)	135
Table 17: Existing regulations, standards and applications	144
Table 18: Use of scenarios for validation.....	146
Table 19: Network latency performance requirements	147
Table 20: Summary of maximum latency requirements according to ROL.....	148
Table 21: LOXO Alpha technical data	160
Table 22: BFH Smartshuttle technical data	161
Table 23: Summary of parking tests BFH Smartshuttle	168
Table 24: Summary of parking tests LOXO Alpha	169
Table 25: Summary of scenario tests.....	171
Table 26: Cybersecurity test results for Remote Operator Station	179
Table 27: Cybersecurity test results for Remote Vehicle.....	180
Table 28: Cybersecurity test results for communications	180
Table 29: Cybersecurity test results for Remote Operator	180
Table 30: Relevant Research questions from BAST Report.....	186
Table 31: Summary recommendations.....	193

List of Abbreviations

ALKS	Automated Lane Keeping System
ANSI	American National Standards Institute
5GAA	5G Automotive Association
ADS	Automated Driving System
AEB	Automated Emergency Braking
AEBS	Automated Emergency Braking System
AFNOR	French Association for Standardization
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AP	Attack Path
AR	Augmented Reality
AV	Automated Vehicle
BASt	Bundesamt für Strassenwesen / Federal Highway Research Institute
BSI	British Standards Institution
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CLEPA	European Association of Automotive Suppliers
CMS	Camera Monitoring System
CR	Cybersecurity Requirements
CRA	Cyber Resilience Act
DDOS	Distributed Denial of Service
DDT	Dynamic Driving Task
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DGNSS	Differential Global Navigation Satellite System
DIN	Deutsches Institut für Normung / German Institute for Standardization
DLR	Deutsches Zentrum für Luft- und Raumfahrt / German Aerospace Centre
DSSAD	Data storage systems for automated driving vehicles
E/E	Electrical and Electronic
EDR	Event Data Recorder
EN	European Standard
EU	European Union
FEDRO	Federal Roads Office
FONES	Federal Office for National Economic Supply
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System, GNSS of USA
GRSG	General Safety Provisions Group
GRSP	Passive Safety Group
GRVA	Automated/Autonomous and Connected Vehicles
HMI	Human-Machine Interface

HW	Hardware
ICT	Information and Communications Technology
ID	Unique Identifier
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikations-Technik
IMU	Inertial Measurement Unit
ISA	International Standards on Auditing
ISO	International Organization for Standardization
LMU	Ludwig Maximilian University
LPD	Loi sur la protection des données
LTE	Long Term Evolution
ML	Machine Learning
MRC	Minimal Risk Condition
MRM	Minimal Risk Manoeuvre (system)
NGO	Non-Governmental Organizations
NIS	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
NTRIP	Networked Transport of RTCM via Internet Protocol
OCA	Ordonnance sur la Conduite Automatisée / Ordinance on Automated Driving
ODD	Operation Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OETV	Ordonnance concernant les exigences techniques requises pour les véhicules routiers
OICA	International Organization of Motor Vehicle Manufacturers
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
PAS	Publicly Available Specification
PII	Personally Identifiable Information
RFC	Request for comments
RHIS	Remote Human Input Systems
ROL	Remote Operation Level
RROL	Requirements Remote Operation Level
RSB	Requirements Scenario-Based
RTCM	Radio Technical Commission for Maritime Services
SAAM	Swiss Association for Autonomous Mobility
SAE	Society of Automotive Engineers
SOTIF	Safety Of The Intended Functionality
SwissMoves	Swiss Association of interdisciplinary experts in transport and mobility
TCC	Teleoperation Control Centre
TCS	Time Control System
TGG	Time Glass-to-Glass
ToD	Tele operated Driving
UC	Use Case
UK	United Kingdom

UNECE	United Nations Economic Commission for Europe
UVEK	Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation / Federal Department of the Environment, Transport, Energy and Communications (DETEC)
V2I	Vehicle-to-Infrastructure
VAF	Verordnung über das automatisierte Fahren / Ordinance on Automated Driving
VSS	Schweizerischer Verband der Strassen- und Verkehrsfachleute / Swiss Association of Road and Transport Experts
VTS	Verordnung über die technischen Anforderungen an Strassenfahrzeuge / Ordinance on Technical Requirements
WP	Workpackage

Zusammenfassung

Beschreibung des Problems

Der weltweite Übergang zur automatisierten Mobilität hat zu bedeutenden Fortschritten bei den Technologien für automatisierte Fahrzeuge (AV) geführt. Pilotprojekte auf internationaler Ebene, aber auch in der Schweiz, haben das Potenzial von AVs für verschiedene Anwendungen wie die Anbindung an den öffentlichen Nahverkehr und die Warenlieferung gezeigt. In der Schweiz haben Organisationen wie **SAAM** (Swiss Association for Autonomous Mobility) [1] und **SwissMoves** [2] eine zentrale Rolle bei der Förderung der Zusammenarbeit zwischen Industrie, Wissenschaft und Behörden. Diese Organisationen unterstützen nicht nur die Entwicklung und Umsetzung von wegweisenden Projekten, sondern dienen auch als wichtige Plattformen für die Verbreitung von Wissen und die Förderung von Innovationen auf dem Gebiet der automatisierten und vernetzten Mobilität.

In der Schweiz ist zum Zeitpunkt der Erstellung dieses Berichts im Jahr 2024 die Anwesenheit eines qualifizierten Bedieners an Bord von AVs vorgeschrieben, der in kritischen Situationen die Kontrolle übernimmt. Diese Anforderung schränkt die wirtschaftliche Tragfähigkeit des AV-Betriebs ein. Das Bundesamt für Strassen (ASTRA) hat am 18. Oktober 2023 ein Vernehmlassungsverfahren zur Erarbeitung eines neuen Rechtsrahmens eröffnet [3], die mit der Verabschiedung der "Ordonnance sur la conduite automatisée" (**OCA**) / "Verordnung über das automatisierte Fahren" (**VAF**) durch den Bundesrat am 13. Dezember 2024 abgeschlossen wurde [4]. Diese Verordnung [5], die am 1. März 2025 in Kraft treten soll, legt umfassende betriebliche Anforderungen für führerlose Fahrzeuge mit einem Automatisierungssystem (**AV**) fest. Gemäss dieser Verordnung müssen diese AVs von einem Operator überwacht werden, der aus der Ferne eingreifen kann, wenn das Fahrzeug auf eine Situation stösst, die es nicht autonom lösen kann.

Der Einsatz von AVs, insbesondere für den öffentlichen Nahverkehr und den Gütertransport auf der letzten Meile, wird als praktikable Lösung zur Bewältigung aktueller betrieblicher Herausforderungen angesehen. Systeme für den Fernbetrieb (**Remote Operation Systems**) ermöglichen die wirtschaftliche Durchführbarkeit, indem sie Ferninterventionen erleichtern und die Lücke schliessen, wo eine vollständige Automatisierung noch nicht möglich ist.

Die technischen Möglichkeiten für Remote Operation Systems haben sich erheblich weiterentwickelt. Moderne Systeme integrieren nun fortschrittliche Sensoren, Kameras und Datenkommunikationstechnologien, die eine Überwachung und Steuerung in Echtzeit ermöglichen. Um jedoch ein verlässliches Zulassungsverfahren für diese Remote Operation Systems zu etablieren, müssen umfassende und robuste Anforderungen definiert werden, die die Verkehrssicherheit, die IT-Sicherheit, den Datenschutz, die Cybersecurity-Resilienz und die Ausbildung der Betreiber umfassen. Das vom ASTRA in Auftrag gegebene Forschungsprojekt adressiert diese Herausforderungen, indem es aufbauend auf nationaler und internationaler

Forschung Mindestanforderungen für Remote Operation Systems definiert und validiert. Durch die Nutzung des Fachwissens aus dem ersten Teleoperationszentrum der Schweiz [6] [7] und anderen Pilotprojekten stellt dieses interdisziplinäre Projekt sicher, dass es mit den sich entwickelnden technologischen und regulatorischen Gegebenheiten Schritt hält und gleichzeitig hohe Sicherheits- und Zuverlässigkeitsstandards erfüllt. Ein besonderer Schwerpunkt lag auf der Gewährleistung der Cybersicherheit durch regelmässige Tests, Überwachung und Anpassung an internationale Standards.

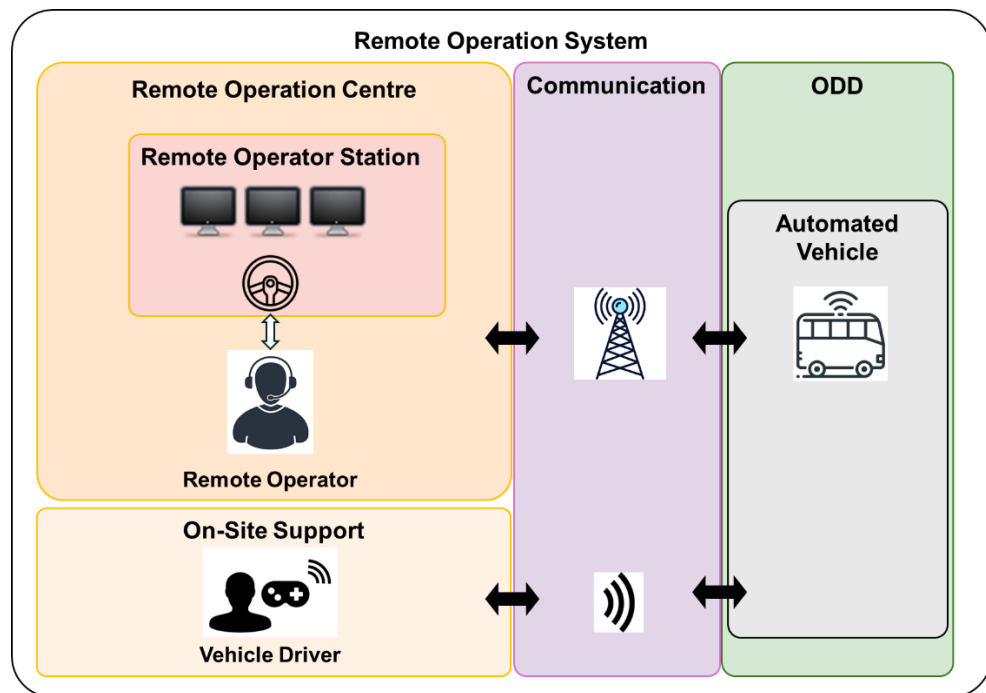


Fig-Z 1: Überblick über ein System für den Fernbetrieb (Remote Operation System)

Zielsetzungen

Das Forschungsprojekt befasst sich mit der zentralen Herausforderung sicherzustellen, dass das Remote Operation System hohe Sicherheits- und Zuverlässigkeitsstandards erfüllen, und zielt gleichzeitig darauf ab, technologische und regulatorische Fortschritte voranzutreiben. Um dies zu erreichen, verfolgte das Projekt zwei Hauptziele:

1. Definieren der Mindestanforderungen an die Verkehrssicherheit, den Verkehrsfluss und die IT-Sicherheit für ein Remote Operation System:

Ziel des Projekts war es, eine umfassende Reihe von Sicherheits-, Cybersicherheits- und Betriebsanforderungen für Remote Operation Systems festzulegen. Diese Anforderungen dienen als Grundlage für die Bewertung, Genehmigung und Betrieb solcher Systeme. Zu den wichtigsten Aspekten gehören:

- **Operational Design Domain (ODD):** Berücksichtigung der Infrastruktur, der Wetterbedingungen und der Interaktion mit anderen Verkehrsteilnehmern
- **Automated Vehicle (AV):** Spezifikation von Technologien für die Perzeption, Sensoren und Aktoren, die für einen zuverlässigen Betrieb entscheidend sind
- **Kommunikation:** Fokus auf IT-Sicherheit, Latenzmanagement, Redundanz und Zuverlässigkeit, um einen stabilen Datenaustausch zu gewährleisten
- **Remote Operator Station:** Entwicklung fortschrittlicher Visualisierungs- und Audiottechnologien zur Verbesserung der Interaktion des Operators mit AVs
- **Remote Operator:** Definition von Ausbildungsstandards und Schlüsselkompetenzen, die für einen effektiven und sicheren Systembetrieb erforderlich sind

2. Bereitstellung der Grundlage für ein besseres Verständnis der Grenzen von Remote-Operation-Systemen und die Ableitung von Anforderungen für deren Bewertung und Zulassung

Um die Integration und Regulierung von Remote Operation Systemen zu unterstützen, konzentrierte sich das Projekt auf die Identifizierung ihrer Einsatzgrenzen und die Ableitung von Kriterien für ihre Bewertung und Genehmigung. Dies beinhaltete:

- **Abgleich der Anforderungen** an internationale Standards und nationale Regelwerke, um Konsistenz und Skalierbarkeit zu gewährleisten
- **Validierung von Anforderungen** durch eine Kombination aus theoretischen Analysen, experimentellen Tests und Szenariobewertungen, um ihre Anwendbarkeit in realen Kontexten zu gewährleisten

Es ist zu beachten, dass das Projekt speziell auf führerlose Fahrzeuge mit der Automatisierungsstufe 4 oder 5 (ISO/SAE PAS 22736, 2021) abzielt, da diese Stufen die notwendige Basis für ein Remote Operation System darstellen. Diese Fahrzeuge sind zwar in der Lage, die meisten Fahraufgaben automatisch zu erledigen, sind jedoch auf die Unterstützung durch einen Operator angewiesen, um einen sicheren und zuverlässigen Betrieb in Szenarien zu gewährleisten, in denen eine vollständige Automatisierung noch nicht möglich ist

Methodik

Um eine solide Grundlage für Remote Operation Systems zu schaffen, wurde im Rahmen des Projekts ein systematischer und multidisziplinärer Ansatz gewählt, der Praxistests, Konsultationen von Interessengruppen und die Einhaltung etablierter Standards umfasst. Die Methodik umfasste die folgenden Schlüsselemente:

1. Entwicklung von Szenarien und Definition einer Taxonomie

Es wurden acht repräsentative Szenarien erstellt, um reale Herausforderungen zu simulieren, wie z. B. Netzunterbrechungen, ungünstige Wetterbedingungen und komplexe städtische Verkehrsverhältnisse. Diese Szenarien boten einen strukturierten Rahmen für die Bewertung der Leistungsfähigkeit des Remote Operation System unter verschiedenen Betriebsbedingungen und dienten als Grundlage für die Definition der Fernbedienstufen (**Remote Operation Level, ROL**). Aufbauend auf dem Rahmenwerk von DriveU.auto entwickelte das Projekt eine umfassende Taxonomie von fünf Remote Operation Level (ROL₁-ROL₅).

2. Definition der Anforderungen

Im Rahmen der Methodik hat das Projektteam die definierten Anforderungen systematisch in drei Hauptkategorien eingeteilt:

- **ROL-basierte Anforderungen:** Berücksichtigung der spezifischen Bedürfnisse und Rollen von Operatoren auf verschiedenen Remote Operation Levels
- **Szenariobasierte Anforderungen:** Konzentriert auf die Bewältigung operativer Herausforderungen unter verschiedenen realen Bedingungen
- **Anforderungen an die Cybersicherheit:** Sicherstellung eines soliden Schutzes vor externen und internen Bedrohungen, der die Integrität der Daten, die Zuverlässigkeit des Netzes und die Widerstandsfähigkeit des Systems umfasst

3. Validierungsansätze

Um die Zuverlässigkeit und Anwendbarkeit der festgelegten Anforderungen zu gewährleisten, wurden drei sich ergänzende Validierungsmethoden angewandt:

- **Angleichung an internationale Normen und rechtliche Rahmenbedingungen:** Sicherstellung der Anpassung an internationale Vorschriften wie UNECE, ISO-Normen und die neue OCA/VAF-Verordnung der Schweiz
- **Szenariobasierte Validierung:** Prüfung der Anforderungen anhand der ausgewählten Szenarien zur Bestätigung ihrer Relevanz und Anwendbarkeit
- **Theoretische und experimentelle Tests:** Bewertung der Auswirkungen von Netzwerklatenz, Hinderniserkennungsfähigkeiten und anderen kritischen Faktoren durch Testfahrten vor Ort und Simulationen

4. Validierung der Cybersicherheit

Die Cybersicherheit war ein zentrales Thema, und dazu wurden 193 spezifische Anforderungen zum Schutz des Remote Operation System definiert. Diese Anforderungen betrafen Bedrohungen für das AV, die Kommunikationskanäle und die Fernbedienungsstation (Remote Operation Station). Zu den Validierungsaktivitäten gehörte eine rigorose Penetrationstestkampagne, die sicherstellt, dass die definierten

Cybersicherheitsmassnahmen sowohl praktisch als auch effektiv getestet werden können.

5. Engagement der Interessengruppen

Workshops und Interviews mit Branchenexperten, Regierungsbehörden und akademischen Forschern lieferten unschätzbare Erkenntnisse. Diese Zusammenarbeit bereicherte die Projektergebnisse und stellte sicher, dass sie für die Herausforderungen der Praxis relevant sind und mit den Anforderungen künftiger Remote Operation Systems übereinstimmen.

Rechtliche Rahmenbedingungen und Normen

Die regulatorische Landschaft für automatisierte und aus der Ferne betriebene Fahrzeuge ist komplex (siehe Abbildung unten), und die Integration dieser Fahrzeuge wird durch sich entwickelnde internationale und nationale Normen geprägt. Zwei zentrale internationale Rechtsakte, das **Genfer Übereinkommen über den Strassenverkehr** (1949) [8] und das **Wiener Übereinkommen über den Strassenverkehr** (1968, geändert 2016/2021) [9], dienen als grundlegende Verträge, die die Verantwortung des Fahrers regeln und den Fernbetrieb unter bestimmten Bedingungen ermöglichen. Ergänzt werden diese Übereinkommen durch **UNECE-Verordnungen** wie die Verordnung **Nr. 155 Cybersecurity** [10] und die Verordnung **Nr. 156 Software-Updates** [11], die detaillierte technische Anforderungen zur Gewährleistung der Systemsicherheit und Interoperabilität enthalten.

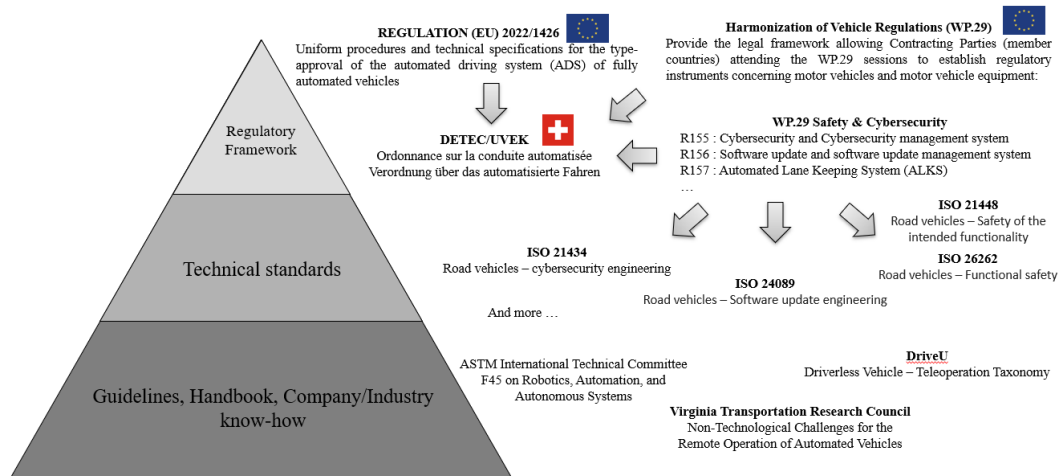


Fig-Z 2: Übersicht über Vorschriften, Normen und Richtlinien

In der **Schweiz** hat der Bundesrat am 18. Oktober 2023 ein Vernehmlassungsverfahren zur Einführung der **OCA/VAF-Verordnung** eröffnet. Die Verordnung wurde vom Bundesrat am 13. Dezember 2024 verabschiedet und wird am 1. März 2025 in Kraft treten [4]. Mit den folgenden zentralen Bestimmungen sollen umfassende betriebliche Anforderungen für führerlose Fahrzeuge mit einem Automatisierungssystem festgelegt werden:

- **Art. 33:** Vor dem täglichen Betrieb müssen führerlose Fahrzeuge einer Abfahrtskontrolle unterzogen werden, die ein manuelles Fahrmanöver umfasst
- **Art. 34:** Verantwortlichkeiten der Operatoren, einschliesslich der Überwachung der Funktionsfähigkeit der Fahrzeuge, der Steuerung der Automatisierungssysteme und der Einleitung von Sicherheitsmassnahmen in kritischen Situationen. Die Bediener müssen in der Schweiz ansässig sein und die erforderlichen Schulungen absolviert haben
- **Art. 35:** Legt die Anforderungen für die manuelle Bedienung von führerlosen Fahrzeugen fest, wobei betont wird, dass Personen, die das Fahrzeug manuell bedienen, als Fahrer im Sinne der Strassenverkehrsordnung gelten, aber nicht als Operatoren eingestuft werden. Der Wechsel zwischen automatisiertem und manuellem Betrieb ist nur bei Stillstand des Fahrzeugs erlaubt
- **Art. 36:** Anforderungen an den Betreiber oder die Person, die das führerlose Fahrzeug manuell bedient, einschliesslich Fahreignung, Fahrkompetenz, Führerschein, Aus- und Weiterbildung am führerlosen Fahrzeug
- **Art. 37:** Leitlinien für die Schulung des Fahrpersonals, insbesondere im Hinblick auf die technische Funktionsweise des Fahrzeugs und der Automatisierungssysteme
- **Art. 38:** Der Fahrzeughalter muss sicherstellen, dass die Fahrzeuge nur von qualifiziertem Personal betrieben werden und dass technische Wartungs- und Kommunikationsinfrastrukturen vorhanden sind
- **Art. 41:** Verlangt, dass führerlose Fahrzeuge über einen Fahrmodusspeicher verfügen, der die wichtigsten Ereignisse aufzeichnet, einschliesslich der Aktivierung und Deaktivierung des Automatisierungssystems, Manöver zur Risikominimierung, die Kommunikation zwischen dem Fahrzeug und dem Bediener sowie Unterbrechungen der Kommunikationsverbindung
- **Art. 42:** Bei führerlosen Fahrzeugen muss das Automatisierungssystem die Grenzen des zugelassenen Einsatzgebiets erkennen und einhalten
- **Art. 43:** Detaillierte Anforderungen für die Erlangung der Betriebsgenehmigung, einschliesslich der Dokumentation der Feingriffsfähigkeiten und der Zuverlässigkeit der Kommunikation unter definierten Einsatzbedingungen
- **Art. 50:** Das ASTRA wird die Auswirkungen der Verordnung evaluieren, was sich auf künftige Anpassungen und den Forschungsbedarf auswirken kann

Diese Artikel betonen die Bedeutung einer gründlichen Schulung der Operatoren, einer soliden Systemwartung und wirksamer Verfahren zur Risikominderung. Durch die Einbeziehung dieser Bestimmungen soll die OCA/VAF-Verordnung die sichere Integration führerlose Fahrzeuge in öffentliche Strassennetze gewährleisten und gleichzeitig die einzigartigen Herausforderungen angehen, die sich durch solche Technologien ergeben.

Resultate

Das Forschungsprojekt lieferte wichtige Ergebnisse, die die Grundlagen für ein Remote Operation System definieren, wobei der Schwerpunkt auf einer klaren Taxonomie, umfassenden Anforderungen und einer Auswahl von Szenarien für Tests und Validierung lag.

1. Terminologie und Taxonomie

Es wurde eine umfassende Taxonomie (**ROL1-ROL5**) für Fernbedienungsstufen (**Remote Operation Level**) entwickelt, in der die Rollen und Zuständigkeiten von Operatoren und Fahrzeugführern für verschiedene Stufen der Fahrzeugautonomie und -beteiligung klar definiert sind (siehe Abbildung unten). Aufbauend auf dem DriveU.auto-Rahmenwerk wurde diese Taxonomie verfeinert und angepasst, um die in den entwickelten Szenarien ermittelten spezifischen Anforderungen zu erfüllen. Ihre Einfachheit und Flexibilität machen sie zu einem grundlegenden Element sowohl für die Anforderungsdefinition als auch für die Testprozesse in diesem Projekt.

Remote Operation Level	ROL 1	ROL 2	ROL 3	ROL 4	ROL 5
Designation	Remote Controller Driving	Tele Driving	Teleassistance Operation L1	Teleassistance Operation L2	Monitoring
Task	Full control of the vehicle Act like a normal driver Communication	Full control on the vehicle Act like a normal driver Communication	Path drawing Speed control Lights or other control Communication	Path drawing Path confirmation Communication	Supervision Communication
DDT responsibility of operator	Full	Full	Speed application	None	None
OEDR responsibility of operator	Full	None	None	None	None
Remote driver support system active	Collision Avoidance System AEBs*	Collision Avoidance System AEBs*	Vehicle fully automated	Vehicle fully automated	Vehicle fully automated
Responsibility	On-site Operator	Remote Operator	Automated Vehicle	Automated Vehicle	Automated Vehicle
Operator location	< 6 m	On the territory	On the territory	On the territory	On the territory
Speed limitation	6 km/h	6 km/h	Road limitation	Road limitation	Road limitation
Operational safety criteria (MRM trigger)	Remote controller communication	Video latency Driving data command latency	ADS operational Internet connection	ADS operational Internet connection	ADS operational Internet connection
Typical situation	Tele Driving not possible - Bad Internet connection - Bad visibility through camera	Teleassistance L1 not possible - ADS not able to drive autonomously - Complex manoeuvre (e.g. put vehicle at the side of the road)	Teleassistance L2 not possible - Vehicle stationary for too long - Improve traffic flow - Priority agreement situation	Vehicle need confirmation or new path - System limitation - Obstruction on the driving path - Vehicle uncertainty - Complex situation	- Automated Vehicle in normal operation - Part of troubleshooting procedure

*AEBs = Advanced Emergency Braking System
*OEDR = Object and Event Detection and Response

Fig-Z 3: Taxonomie für Fernbedienungsstufen (Remote Operation Level, ROL)

Wie in der nächsten Abbildung dargestellt, unterscheidet diese Taxonomie auch zwischen den Aufgaben der **Teleassistenz**, der **Teleoperation** und des ferngelenkten Fahrens (**Remote Driving**) in Bezug auf die Verantwortlichkeiten des Operators oder des Fahrzeugführers. Die Aufgaben der Teleassistenz (ROL3–5) und der Teleoperation (ROL2) werden vom Operator (Remote Operator) im Fernbedienungs-zentrum (Remote Operation Centre) ausgeführt, der als Fernassistent (**Remote Assistant**) für die Teleassistenz oder als Fernfahrer (**Remote Driver**) für die Teleoperation fungiert. Die manuelle Bedienung (Remote Driving) (ROL1) fällt in den Verantwortungsbereich des Fahrzeugführers (**Vehicle Driver**), der bei Bedarf Unterstützung vor Ort leisten kann.

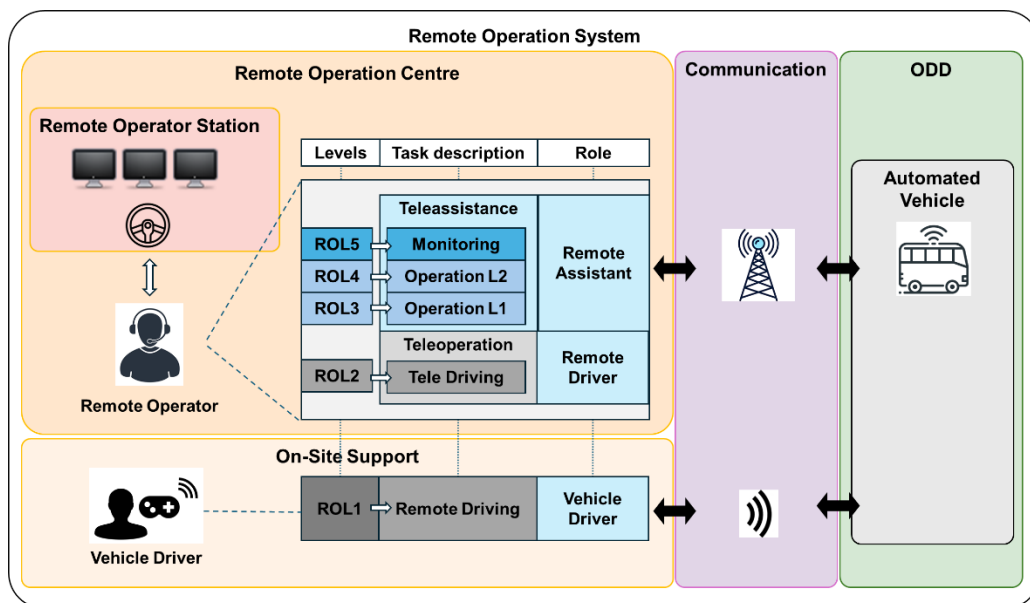


Fig-Z 4: Systeme für den Fernbetrieb (Remote Operation System) mit Aufgaben und Rollen

2. Auswahl der Szenarien

Es wurden acht repräsentative Szenarien ermittelt und analysiert, die sich mit kritischen betrieblichen Herausforderungen befassen, welche in der Praxis auftreten können:

- Szenario 1: Unerwartete Strassensperrung
- Szenario 2: Verlust der Netzwerkverbindung oder schlechte Netzwerkleistung
- Szenario 3: Ungenaue Ortung aufgrund von Problemen mit dem Ortungssystem oder Signalverlust
- Szenario 4: Fehlfunktion des optischen Sensors aufgrund von Sonneneinstrahlung
- Szenario 5: Globales Satellitennavigationssystem (Global Navigation Satellite System - GNSS) und Kilometerzähler liefern aufgrund von rutschiger Strasse nicht eindeutige Ergebnisse
- Szenario 6: Widrige Wetterbedingungen
- Szenario 7: Engpass bei dichtem Verkehr

Diese Szenarien decken eine Vielzahl komplexer Situationen ab, darunter Umweltbedingungen, Netzwerkprobleme und Systemstörungen, und bieten einen strukturierten Rahmen für die Bewertung der Leistungsfähigkeit von einem Remote Operation System.

3. Entwicklung von Anforderungen

Aus einer anfänglichen Datenbank von rund 1.000 Anforderungen, die von den Projektpartnern LOXO, ROSAS/SwissMoves und BFH zur Verfügung gestellt wurden, destillierte das Forschungsteam systematisch einen priorisierten Satz von 247 Anforderungen, die in drei Hauptgruppen unterteilt wurden:

- **ROL-basierte Anforderungen (25):** Berücksichtigung spezifischer Anforderungen und Funktionen für jede ROL, um die Übereinstimmung mit betrieblichen Zielen und Sicherheitsstandards zu gewährleisten
- **Szenariobasierte Anforderungen (29):** Bewältigung von Herausforderungen, die sich aus verschiedenen realen Einsatzsituationen ergeben, z.B. widrige Wetterbedingungen, Sensorfehlfunktionen und Netzunterbrechungen
- **Anforderungen an die Cybersicherheit (193):** Umfassender Schutz vor internen und externen Bedrohungen, Sicherung von Kommunikationskanälen, Systemintegrität und Betriebssicherheit

Dieser verfeinerte Anforderungsrahmen bildet eine solide Grundlage sowohl für die Systementwicklung als auch für behördlichen Genehmigungsverfahren.

4. Validierung und Tests

Um die Anwendbarkeit und Zuverlässigkeit der vorgeschlagenen Anforderungen an das Remote Operation System zu bewerten, wurde im Rahmen des Forschungsprojekts ein vielschichtiger Validierungsansatz angewandt. Dazu gehörten eine szenariobasierte Validierung, Vor-Ort-Tests kritischer Systemfunktionen und rigorose Bewertungen der Cybersicherheit.

a) Szenariobasierte Validierung

Das Forschungsteam entwarf acht repräsentative Szenarien, die reale Herausforderungen widerspiegeln, wie z. B. Netzwerkunterbrechungen, widrige Wetterbedingungen und Sensorfehlfunktionen. Diese Szenarien waren entscheidend für die Bewertung der Anwendbarkeit des Systems und die Prüfung der vorgeschlagenen Anforderungen unter verschiedenen Betriebsbedingungen.

b) Vor-Ort-Tests

Drei verschiedene Kategorien von Vor-Ort-Tests wurden mit den Fahrzeugen LOXO Alpha und BFH Smartshuttle auf der DTC-Teststrecke durchgeführt. Bei jedem Test wurden kritische Aspekte der Funktionsfähigkeit des Systems unter verschiedenen Bedingungen bewertet:

- Bei **Slalomtests** wurde die Manövrierfähigkeit des Systems bei unterschiedlichen Latenzen untersucht. Bei insgesamt 16 Testläufen mit einer Höchstgeschwindigkeit von 6 km/h zeigte sich, dass die vom Operator gesteuerten Fahrzeuge bei Latenzzeiten von bis zu 850 ms die vorgegebene Bahn genau einhielten und bei diesen Werten eine stabile Leistung zeigten. Bei einer höheren Latenz von 1250 ms wurde ein gewisser Rückgang der Präzision beobachtet, der jedoch statistisch nicht signifikant war, was die Robustheit des Systems für den ROL2-Betrieb bei niedrigen Geschwindigkeiten unterstreicht. Die Operatoren bezeichneten die Szenarien mit hoher Latenz als anspruchsvoll, aber mit angemessenem Training zu bewältigen.

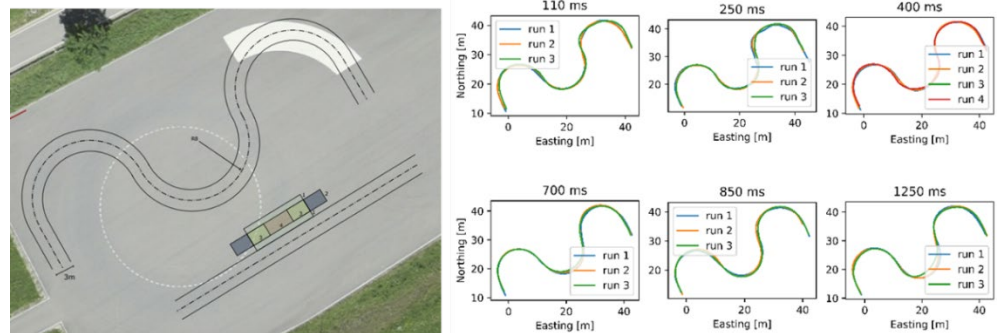


Fig-Z 5: Luftaufnahme der Slalom-Teststrecke vom DTC mit Standortdaten der Slalomtests

- Bei **Einparktests** wurden die Präzision und die Reaktionsfähigkeit des Systems bei langsamen Manövern bewertet. Bei 33 Testläufen meldeten die Operatoren keine spürbaren Latenzeffekte, selbst bei 1000 ms. Die Einparksequenzen wurden anhand der Einhaltung der vorgegebenen Grenzen, der Ausführungsgenauigkeit und der Hindernisvermeidung bewertet. Obwohl die Parkmanöver von Natur aus anspruchsvoll waren, wurde die Latenz nicht als einschränkender Faktor identifiziert, was darauf hindeutet, dass das System in der Lage ist, diese Aufgaben effektiv zu bewältigen.

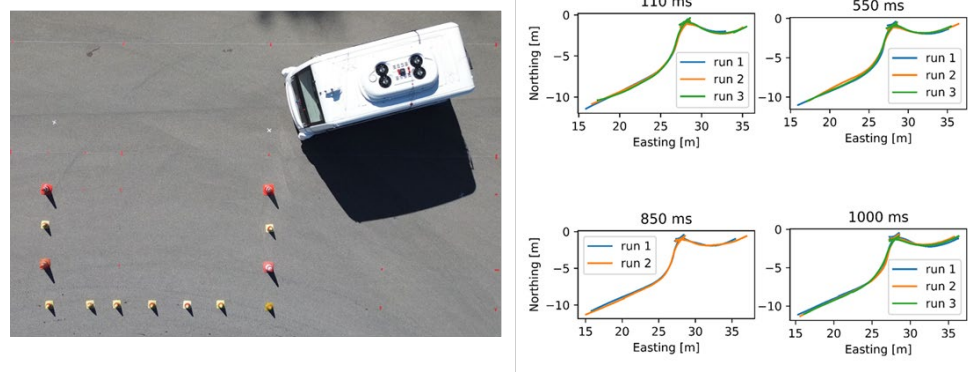


Fig-Z 6: Teststrecke mit Standortdaten der Einparktests

- In den **Tests zu Szenario 8 – "False Positive"-Hinderniserkennung** wurde die Fähigkeit des Systems bewertet, auf falsche Hindernisse zu reagieren, die eine Notbremsung auslösen. Elf Testläufe wurden mit Objekten wie Ästen und Papiertüten durchgeführt, um Fehlalarme zu simulieren. Das automatische Notbremsssystem (AEB) erkannte diese Objekte durchwegs und löste jeweils eine Notbremsung aus. Die Operatoren lösten die Szenarien erfolgreich mit **zwei unterschiedlichen Ansätzen: Umfahren** des Hindernisses und **Überfahren** mit sehr geringer Geschwindigkeit (<1 km/h). Die Ergebnisse bestätigten die Relevanz dieses Szenarios und zeigten, dass das System solche Ereignisse im Rahmen der definierten Anforderungen zuverlässig bewältigen kann.



Fig-Z 7: Szenario 8 – «False positive»-Hinderniserkennung - Lösung unter Umgehung mittels ROL2

c) Validierung der Cybersicherheit

Um einen robusten Schutz gegen interne und externe Bedrohungen zu gewährleisten, wurde eine Teilmenge von 80 der 193 definierten Cybersicherheitsanforderungen rigoros getestet. Die Penetrationstests am LOXO-Alpha-Fahrzeug bestätigten die Einhaltung von Normen wie ISO/IEC 27001:2022 und der UN-Regelung Nr. 155. Obwohl sensible Testergebnisse vertraulich waren, unterstrichen die Tests die Eignung des Systems, strenge Cybersicherheits-Benchmarks zu erfüllen.

d) Wichtigste Ergebnisse

Die wichtigsten Ergebnisse der Validierungsphase dieses Projekts sind:

- **Latenztoleranz:** Es wurde festgestellt, dass Latenzzeiten von bis zu 850 ms bei den für ROL2 typischen niedrigen Geschwindigkeiten (max. 6 km/h) keine nachteiligen Auswirkungen auf die Manövrierfähigkeit haben. Höhere Geschwindigkeiten und andere komplexe Szenarien erfordern weitere Untersuchungen, um mögliche Auswirkungen der Latenz zu ermitteln
- **Relevanz des Szenarios:** Das Szenario "False-positive"-Hinderniserkennung wurde als ein kritisches, reales Problem bestätigt, das mit dem aktuellen Systemdesign lösbar ist
- **Herausforderungen für die Operatoren:** Die Rückmeldungen der Operatoren machten deutlich, wie wichtig es ist, dass sie geschult werden, um mit hohen Latenzzeiten und schwierigen Manövern effektiv umgehen zu können

Empfehlungen

Dieses Forschungsprojekt stellt einen bedeutenden Meilenstein bei der Weiterentwicklung von Remote Operation System mit AVs dar, indem es sich mit dringenden Herausforderungen befasst und die Grundlage für zukünftige Möglichkeiten der Teleassistenz und Teleoperation schafft. Durch die Entwicklung und Validierung einer umfassenden Taxonomie für Fernbedienungsstufen (Remote Operation Levels - ROLs) und die Definition von Mindestanforderungen schafft das Projekt einen robusten Rahmen für die Gewährleistung von Sicherheit, Zuverlässigkeit und Effizienz bei Fernbetrieb. Der innovative, szenariobasierte Validierungsansatz zeigte die praktische Relevanz der Anforderungen und verdeutlichte die Resilienz dieser Systeme, insbesondere bei niedrigen Geschwindigkeiten und moderaten Latenzzeiten.

Wichtige Erkenntnisse aus den experimentellen Tests, wie die Robustheit des Systems gegenüber Latenzen von bis zu 850 ms (bei der die Höchstgeschwindigkeit des in ROL2 mittels Teleoperation gesteuerten Fahrzeugs 6 km/h nicht überschreiten darf) und die erfolgreiche Bewältigung komplexer Szenarien wie der "False Positive"-Hinderniserkennung, bestätigen die Einsatzfähigkeit von Remote Operation Systems. Gleichzeitig unterstreicht das Projekt Bereiche, die weiterer Erforschung bedürfen, insbesondere die Funktionsfähigkeit des Systems unter verschiedenen Betriebsbedingungen, in städtischen Umgebungen und unter extremen Bedingungen. Die Ergebnisse dieser Forschung unterstreichen die entscheidende Bedeutung von robusten Sicherheitsmassnahmen, der Anpassungsfähigkeit des Systems und der kontinuierlichen Weiterentwicklung von Remote Operation Systems. Diese Mindestanforderungen dienen nicht nur als technische und betriebliche Massstäbe, sondern bilden auch die Grundlage dafür, dass die Systeme eine formelle behördliche Zulassung erhalten können. Die Einhaltung dieser Anforderungen ist für die erfolgreiche Genehmigung, den Betrieb und den breiten Einsatz solcher Systeme von entscheidender Bedeutung.

Um auf diesen Ergebnissen aufzubauen, stimmen die folgenden Empfehlungen mit den in diesem Bericht dargelegten Prioritäten überein:

1. Sicherheit als grundlegendes Prinzip

Die Sicherheit bleibt die zentrale Säule eines Remote Operation System. Bei allen technologischen Fortschritten, regulatorischen Aktualisierungen und betrieblichen Strategien sollte der Schutz aller Verkehrsteilnehmer und Fahrzeuginsassen im Vordergrund stehen. Dazu gehören die Gewährleistung stabiler Kommunikationsverbindungen, Echtzeit-Entscheidungsmöglichkeiten und Redundanzmassnahmen zur Bewältigung unerwarteter Ausfälle.

2. Verfeinerung und Erweiterung von Szenario-Definitionen

Ständige Aktualisierungen der Szenario-Definitionen sind von entscheidender Bedeutung, da sie Erkenntnisse aus realen Anwendungen einbeziehen. Neben der Verfeinerung bestehender Szenarien ist es von entscheidender Bedeutung, neue Szenarien zu entwickeln, die auf neue betriebliche Herausforderungen wie höhere Fahrzeuggeschwindigkeiten, komplexe städtische Umgebungen und ungünstige

Wetterbedingungen eingehen. Auf diese Weise wird sichergestellt, dass die Szenarien umfassend und auf die sich entwickelnden Anforderungen von Remote Operation Systems abgestimmt bleiben.

3. Technologische Entwicklung und Anpassung an neue Normen

Da sich die Remote-Betriebs- und Kommunikationstechnologien weiterentwickeln, sind regelmässige Überprüfungen und Aktualisierungen der festgelegten Anforderungen unerlässlich. Diese Aktualisierungen sollten Fortschritte in Bereichen wie 5G-Konnektivität, adaptive Datenstreaming-Strategien und dynamische Ressourcenzuweisung einbeziehen. Diese Innovationen werden die Nutzung der Uplink-Bandbreite optimieren, die Skalierbarkeit für den Betrieb grosser Flotten unterstützen und die Betriebszuverlässigkeit verbessern. Rückmeldungen aus realen Anwendungen und die Anpassung an neue internationale Vorschriften werden diese Anforderungen weiter verfeinern.

4. Verbesserungen für die Teleoperation (ROL2)

Spezifische Verbesserungen für den ROL2-Betrieb sind erforderlich, um einen nahtlosen Eingriff bei niedrigen Geschwindigkeiten (≤ 6 km/h) zu gewährleisten. Die Forschung sollte sich auf die Verbesserung der Schnittstellen für die Operatoren, die genauere Untersuchung der Auswirkungen von Latenzzeiten (z.B. Auswirkungen schwankender Latenzzeiten) und die Verbesserung der Reaktionsfähigkeit des Systems konzentrieren, um den Anforderungen direkter Kontrollszenarien gerecht zu werden, und die ergonomischen, psychologischen und kognitiven Anforderungen der Operatoren sowohl für die Teleoperation als auch für die Teleassistenz zu berücksichtigen.

5. Regelmässige Überprüfung und Weiterentwicklung

Der dynamische Charakter der automatisierten Mobilität erfordert eine regelmässige Neubewertung sowohl der technischen Normen als auch der betrieblichen Rahmenbedingungen. Diese regelmässigen Überprüfungen sollten sich mit neuen Herausforderungen befassen, technologische Durchbrüche einbeziehen und die Auswirkungen von Änderungen der Rechtsvorschriften auf die Systemgestaltung und -einführung bewerten.

6. Schulung und Zertifizierung für Operatoren

Umfassende Schulungsprogramme für Operatoren sind von entscheidender Bedeutung. Diese Programme sollten praktische Simulationen von Notfallszenarien, eingehende Kenntnisse der Fahrzeugsysteme und ein klares Verständnis der geltenden Verkehrsvorschriften beinhalten. Zertifizierungsverfahren müssen sicherstellen, dass die Operatoren die höchsten Standards für Kompetenz und Vorbereitung erfüllen.

7. Angleichung an internationale Normen

Die Harmonisierung der nationalen Anforderungen mit internationalen Normen wie der UN-Regelung Nr. 46 und der ISO-Norm 16505:2019 ist für die Gewährleistung der Interoperabilität und der globalen Anwendbarkeit von entscheidender Bedeutung. Regelmässige Aktualisierungen zur Anpassung an Fortschritte bei Kamera-Monitoring-Systemen, Latenz-Benchmarks und

Sicherheitsvorschriften unterstützen die einheitliche Umsetzung in verschiedenen Rechtsordnungen.

Zukunft und praktische Anwendungen

Die Ergebnisse des Projekts und das entwickelte Fachwissen machen das Konsortium zu einer wertvollen Ressource für die Unterstützung der Umsetzung der OCA/VAF-Verordnung, die am 18. Oktober 2023 im Rahmen eines Vernehmlassungsverfahrens eingeführt [3] und vom Bundesrat am 13. Dezember 2024 verabschiedet wurde [4]. Dieses Forschungsprojekt befasst sich direkt mit den wichtigsten Bestimmungen in Kapitel 5 der OCA/AFV-Verordnung [5], um die Betriebsbereitschaft und Sicherheit von führerlosen Fahrzeugen zu gewährleisten. Die im Rahmen des Projekts entwickelte Terminologie und Taxonomie für Fernbedienungsstufen (ROL), sind wesentliche Instrumente zur Klärung der Verantwortlichkeiten und zur Einhaltung des neuen Rechtsrahmens.

Durch die Nutzung seiner soliden Wissensbasis bei der Definition und Validierung von Mindestanforderungen für Systeme für den Fernbetrieb (Remote Operation System) könnte das Konsortium Bundesbehörden bei der Bewertung für die Zulassung und Betrieb solcher Systeme unterstützen. Dazu gehören die Durchführung technischer Bewertungen, die Unterstützung des Genehmigungsverfahrens und die Bereitstellung von Schulungs- und Beratungsdiensten. Diese Bestrebungen schliessen die Lücke zwischen den gesetzlichen Anforderungen und dem praktischen Einsatz und gewährleisten somit die sichere und effiziente Integration von führerlosen Fahrzeugen (AVs) in das öffentliche Strassennetz [12] [13]. Diese Aufgabe ist angesichts der Herausforderungen, die eine Integration von Systemen für den Fernbetrieb (Remote Operation System) in einen sich rasch entwickelnde technologische und rechtliche Landschaft mit sich bringt, besonders wichtig. Die im Rahmen des Projekts definierten Anforderungen stellen eine Momentaufnahme der aktuellen Fähigkeiten dar und müssen regelmässig aktualisiert werden, um Fortschritten, Änderungen der internationalen Normen und sich weiterentwickelnden Vorschriften Rechnung zu tragen.

Als Vermittler zwischen manuellem und vollautomatisiertem Fahren sind Teleoperation und Teleassistenz entscheidende Technologien für den Übergang zur automatisierten Mobilität. Diese Systeme erleichtern die Schliessung betrieblicher Lücken bei der Einführung und Nutzung führerlose Fahrzeuge (AVs), insbesondere in Szenarien, in denen eine vollständige Automatisierung noch nicht möglich ist. Darüber hinaus könnte das Konsortium die Zusammenarbeit zwischen Behörden, Branchenvertretern und Forschungseinrichtungen fördern und so die sichere und effiziente Integration von führerlosen Fahrzeugen in das schweizerische Verkehrsnetz unterstützen.

Résumé

Description du problème

La transition mondiale vers la mobilité automatisée a conduit à des avancées significatives dans les technologies des véhicules automatisés (AV). Des projets pilotes à l'échelle internationale, mais aussi en Suisse, ont démontré le potentiel des AV dans diverses applications, telles que les liaisons de transport public du dernier kilomètre et la livraison de marchandises. En Suisse, des organisations comme **SAAM** (Swiss Association for Autonomous Mobility) [1] et **SwissMoves** [2] jouent un rôle central dans la promotion de la collaboration entre l'industrie, les universités et les autorités publiques. Ces organisations soutiennent non seulement le développement et la mise en œuvre de projets de pointe, mais servent également de plateformes clés pour la diffusion des connaissances et la promotion de l'innovation dans le domaine de la mobilité automatisée et connectée.

En Suisse, au moment de la rédaction de ce rapport en 2024, le code de la route impose la présence d'un opérateur qualifié à bord des AV pour prendre le contrôle dans les situations critiques. Cette exigence limite la viabilité économique des opérations des AV. L'Office fédéral des routes (OFROU) a lancé, le 18 octobre 2023, une consultation pour élaborer un nouveau cadre juridique [3], débouchant sur l'adoption par le Conseil fédéral, le 13 décembre 2024, de l'« Ordonnance sur la conduite automatisée » (**OCA**) / « Verordnung über das automatisierte Fahren » (**VAF**) [4]. Cette ordonnance [5], qui doit entrer en vigueur le 1er mars 2025, établit des exigences opérationnelles complètes pour les véhicules sans conducteur équipés d'un système d'automatisation (**AV**). Selon cette ordonnance, ces AV doivent être surveillés par un opérateur, qui peut intervenir à distance lorsque le véhicule rencontre une situation qu'il ne peut résoudre de manière autonome.

Le déploiement d'AV, en particulier pour les opérations de transport public et le transport de marchandises sur le dernier kilomètre, est considéré comme une solution viable pour relever les défis opérationnels actuels. Les systèmes d'opérations à distance (**Remote Operation Systems**) permettent la faisabilité économique en facilitant les interventions à distance, comblant ainsi les lacunes là où l'automatisation complète n'est pas encore réalisable.

Les capacités techniques des Remote Operation Systems ont considérablement progressé. Les systèmes modernes intègrent désormais des capteurs avancés, des caméras et des technologies de communication de données, permettant une surveillance et un contrôle en temps réel. Cependant, pour établir un processus d'approbation fiable pour ces Remote Operation System, des exigences complètes et solides doivent être définies, englobant la sécurité routière, la sécurité informatique, la protection des données, la résilience en matière de cybersécurité et la formation des opérateurs. Le projet de recherche commandé par l'OFROU répond à ces enjeux en

définissant, sur la base de recherches nationales et internationales, les exigences minimales pour les Remote Operation Systems, puis en les validant. En s'appuyant sur l'expertise acquise par le premier centre de téléopération de Suisse [6] [7] et d'autres projets pilotes, cet effort interdisciplinaire permet de s'aligner sur les évolutions technologiques et réglementaires tout en respectant des normes élevées de sécurité et de fiabilité. Un accent particulier a été mis sur la résilience de la cybersécurité grâce à des tests réguliers, à la surveillance et à l'alignement sur les normes internationales.

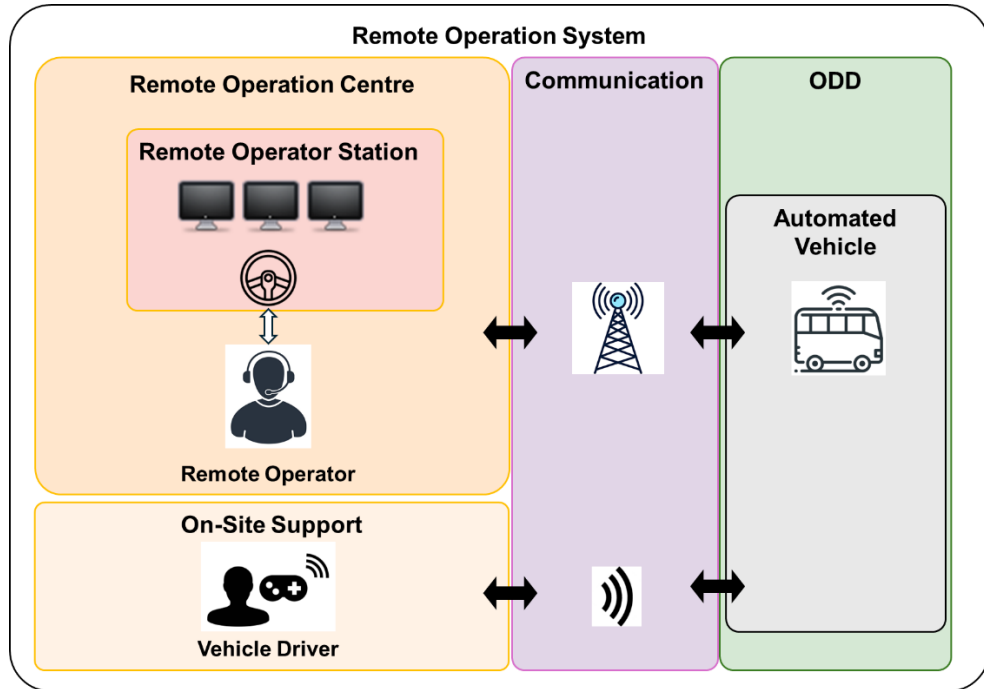


Fig-R 1: Vue d'ensemble système d'opération à distance (Remote Operation Systems)

Objectifs

Le projet de recherche aborde le défi central de garantir que les systèmes de fonctionnement à distance répondent à des normes élevées de sécurité et de fiabilité, tout en visant à promouvoir les progrès technologiques et réglementaires. Pour y parvenir, le projet a poursuivi deux objectifs principaux :

1. Définir les exigences minimales en matière de sécurité routière, de fluidité du trafic et de sécurité informatique pour un Remote Operation System :

Le projet visait à établir un ensemble complet d'exigences en matière de sécurité, de cybersécurité et d'exploitation pour le Remote Operation System. Ces exigences servent de base à l'évaluation, à l'homologation et au fonctionnement de ces systèmes. Les principaux aspects sont les suivants :

- **Operational Design Domain (ODD):** Prise en compte de l'infrastructure, des conditions météorologiques et des interactions avec les autres usagers de la route
- **Automated Vehicle (AV):** Spécification des technologies de perception, des capteurs et des actionneurs, essentiels pour un fonctionnement fiable
- **Communication:** Accent mis sur la sécurité informatique, la gestion des temps de latence, la redondance et la fiabilité, afin de garantir un échange de données stable
- **Remote Operator Station:** Développement de technologies avancées de visualisation et d'audio pour améliorer l'interaction de l'opérateur avec les véhicules automatisés (AV)
- **Remote Operator:** Définition des normes de formation et des compétences clés requises à une exploitation sûre et efficace du système

2. Fournir une base pour mieux comprendre les limites des Remote Operation Systems et en déduire des exigences pour leur évaluation et leur approbation.

Pour soutenir l'intégration et la réglementation des Remote Operation System, le projet s'est concentré sur l'identification de leurs limites opérationnelles et sur l'élaboration de critères d'évaluation et d'approbation. Cela inclut :

- **L'alignement des exigences** sur les normes internationales et les cadres réglementaires nationaux pour garantir la cohérence et l'évolutivité
- **La validation des exigences** par une combinaison d'analyses théoriques, d'essais expérimentaux et d'évaluations de scénarios, afin de garantir leur applicabilité dans des contextes réels

Il faut noter que le projet vise spécifiquement les véhicules dont le niveau d'automatisation de la conduite est de 4 ou 5 (ISO/SAE PAS 22736, 2021), car ces niveaux constituent la base nécessaire pour un Remote Operation System. Bien que ces véhicules soient capables de gérer la plupart des tâches de conduite de manière automatisée, ils s'appuient sur un opérateur pour fonctionner de manière sûre et fiable dans des scénarios où l'automatisation complète n'est pas encore possible.

Méthodologie

Afin de garantir une base solide pour les Remote Operation System, le projet a adopté une approche systématique et multidisciplinaire, intégrant des tests en conditions réelles, des consultations des parties prenantes et le respect des normes établies. La méthodologie comprenait les éléments clés suivants :

1. Élaboration de scénarios et définition d'une taxonomie

Huit scénarios représentatifs ont été créés pour simuler les défis du monde réel, tels que les perturbations du réseau, les conditions météorologiques défavorables et les complexités du trafic urbain. Ces scénarios ont fourni un cadre structuré pour l'évaluation des performances du Remote Operation System dans des conditions opérationnelles variées et ont servi de base à la définition des niveaux d'opération à distance, (**Remote Operation Levels, ROL**). En s'appuyant sur le cadre proposé par DriveU.auto, le projet a développé une taxonomie complète de cinq Remote Operation Level (ROL1-ROL5).

2. Définition des exigences

Dans le cadre de la méthodologie, l'équipe de projet a systématiquement regroupé les exigences définies en trois catégories principales :

- **Exigences basées sur le ROL** : Répondre aux besoins et rôles spécifiques des opérateurs avec différents Remote Operation Level
- **Exigences basées sur des scénarios** : Elles sont axées sur la résolution des problèmes opérationnels dans diverses conditions réelles
- **Exigences en matière de cybersécurité** : Assurer une protection solide contre les menaces externes et internes, couvrant l'intégrité des données, la fiabilité du réseau et la résilience du système

3. Approches de validation

Trois méthodes de validation complémentaires ont été utilisées pour garantir la fiabilité et l'applicabilité des exigences définies :

- **Alignement sur les normes internationales et les cadres réglementaires** : Assurer l'alignement sur les réglementations internationales telles que la CEE-ONU, les normes ISO et la nouvelle ordonnance OCA/VAF de la Suisse
- **Validation basée sur des scénarios** : Tester les exigences par rapport aux scénarios sélectionnés afin de confirmer leur pertinence et leur applicabilité
- **Essais théoriques et expérimentaux** : Évaluation de l'impact de la latence du réseau, des capacités de détection des obstacles et d'autres facteurs critiques par le biais de tests et de simulations sur site

4. Validation de la cybersécurité

La cybersécurité était au centre des préoccupations, 193 exigences spécifiques ayant été définies pour protéger le Remote Operation System. Ces exigences portaient sur les menaces pesant sur l'AV, les canaux de communication et la station d'opération à distance (Remote Operation Station). Les activités de validation comprenaient une campagne rigoureuse de tests de pénétration, garantissant que les mesures de cybersécurité définies peuvent être testées de manière pratique et efficace.

5. Engagement des parties prenantes

Des ateliers et des entretiens avec des experts de l'industrie, des régulateurs et des chercheurs universitaires ont permis d'obtenir des informations précieuses. Cette collaboration a permis d'enrichir les conclusions du projet, en garantissant leur pertinence par rapport aux défis du monde réel et leur alignement sur les besoins des futurs Remote Operation Systems.

Cadres juridiques et normes

Le paysage réglementaire des véhicules automatisés et opérés à distance est complexe (voir figure ci-dessous), l'évolution des normes internationales et nationales façonnant leur intégration. Deux actes juridiques internationaux essentiels, la **Convention de Genève sur la circulation routière** (1949) [8] et la **Convention de Vienne sur la circulation routière** (1968, amendée 2016/2021) [9], servent de traités fondamentaux, qui traitent des responsabilités du conducteur et autorisent les opérations à distance sous certaines conditions. Ces conventions sont complétées par des **règlements de la CEE-ONU**, tels que le règlement n° 155 **Cybersecurity** [10] et le règlement n° 156 **Software-Updates** [11], qui fournissent des exigences techniques détaillées pour garantir la sécurité et l'interopérabilité des systèmes.

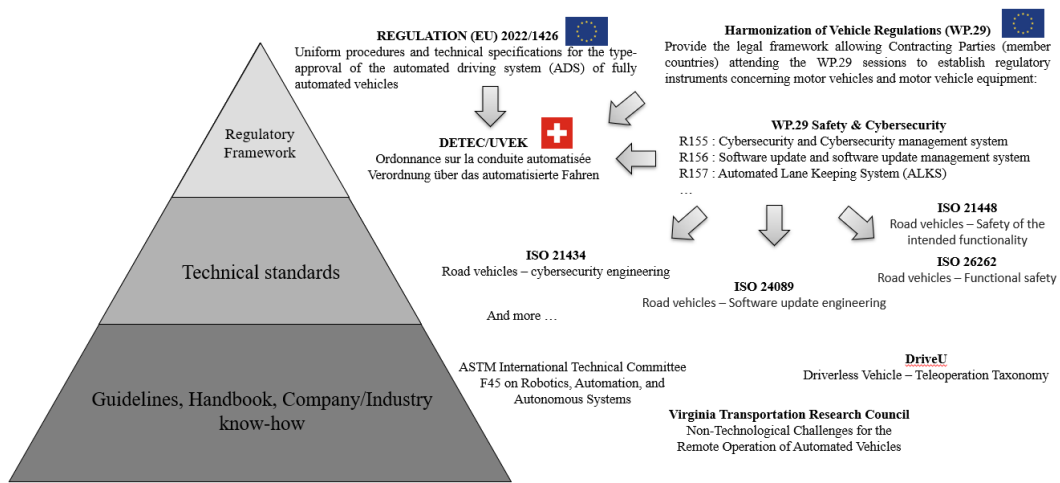


Fig-R 2: Aperçu des règlements, normes et lignes directrices

En **Suisse**, le Conseil fédéral a lancé, le 18 octobre 2023, une procédure de consultation en vue de l'introduction de l'**ordonnance OCA/VAF**. L'ordonnance a été adoptée par le Conseil fédéral le 13 décembre 2024 et entrera en vigueur le 1er mars 2025 [4]. Les principales dispositions suivantes visent à établir des exigences opérationnelles complètes pour les véhicules sans conducteur équipés d'un système d'automatisation:

- **Art. 33** : Avant leur mise en service quotidienne, les véhicules sans conducteur doivent faire l'objet d'un contrôle de départ impliquant une manœuvre de conduite manuelle
- **Art. 34** : Responsabilités des opérateurs, y compris la surveillance du bon fonctionnement des véhicules, la gestion des systèmes d'automatisation et la mise en œuvre de mesures de sécurité dans les situations critiques. Les opérateurs doivent être basés en Suisse et avoir suivi les formations requises
- **Art. 35** : Spécifie les exigences relatives à la conduite manuelle des véhicules sans conducteur, en soulignant que les personnes qui conduisent manuellement le véhicule sont considérées comme des conducteurs au sens de la loi sur la circulation routière, mais ne sont pas considérées comme des opérateurs. Les transitions entre les modes automatisé et manuel ne sont autorisées que lorsque le véhicule est à l'arrêt
- **Art. 36** : Exigences applicables à l'exploitant ou à la personne qui conduit manuellement le véhicule sans conducteur, y compris l'aptitude à la conduite, la compétence de conduite, le permis de conduire, la formation et le perfectionnement sur le véhicule sans conducteur
- **Art. 37** : Lignes directrices pour la formation des opérateurs, notamment en ce qui concerne le fonctionnement technique du véhicule et des systèmes d'automatisation
- **Art. 38** : Obligation pour les propriétaires de véhicules de s'assurer que les véhicules ne sont conduits que par du personnel qualifié et que des infrastructures d'entretien technique et de communication sont en place
- **Art. 41** : Obligation pour les véhicules sans conducteur de disposer d'un enregistreur de mode de conduite qui enregistre les principaux événements, notamment l'activation et la désactivation du système d'automatisation, les manœuvres de réduction des risques, la communication entre le véhicule et l'opérateur et les interruptions du lien de communication
- **Art. 42** : Dans le cas des véhicules sans conducteur, le système d'automatisation doit reconnaître et respecter les limites de la zone d'utilisation approuvée
- **Art. 43** : Exigences détaillées pour l'obtention d'une autorisation opérationnelle, y compris la documentation sur les capacités d'intervention à distance et la fiabilité des communications dans des conditions d'utilisation définies
- **Art. 50** : L'OFROU évaluera les effets de l'ordonnance, ce qui pourrait influencer les ajustements futurs et les exigences en matière de recherche

Ces articles soulignent l'importance d'une formation rigoureuse des opérateurs, d'une maintenance robuste des systèmes et de procédures efficaces de réduction des risques. En intégrant ces dispositions, le règlement OCA/VAF vise à garantir l'intégration sûre des véhicules sans conducteur dans les réseaux routiers publics, tout en relevant les défis uniques posés par ces technologies.

Résultats

Le projet de recherche a produit des résultats importants qui définissent les fondements d'un Remote Operation System, en mettant l'accent sur une taxonomie claire, des exigences complètes et une sélection de scénarios pour les essais et la validation.

1. Terminologie et taxonomie

Une taxonomie complète (**ROL1-ROL5**) des niveaux d'opération à distance (**Remote Operation Level**) a été élaborée, définissant clairement les rôles et les responsabilités des opérateurs et du conducteur du véhicule à différents degrés d'autonomie et d'implication du véhicule (voir figure ci-dessous). S'appuyant sur le cadre DriveU.auto, cette taxonomie a été affinée et adaptée pour répondre aux besoins spécifiques identifiés dans les scénarios élaborés. Sa simplicité et sa flexibilité en font un élément fondamental pour la définition des exigences et les processus d'essai dans ce projet.

On-site Remote Driving
without OEDR sensors Teleoperation
with OEDR sensors ← Teleassistance →

Remote Operation Level	ROL 1	ROL 2	ROL 3	ROL 4	ROL 5
Designation	Remote Controller Driving	Tele Driving	Teleassistance Operation L1	Teleassistance Operation L2	Monitoring
Task	Full control of the vehicle Act like a normal driver Communication	Full control on the vehicle Act like a normal driver Communication	Path drawing Speed control Lights or other control Communication	Path drawing Path confirmation Communication	Supervision Communication
DDT responsibility of operator	Full	Full	Speed application	None	None
OEDR responsibility of operator	Full	None	None	None	None
Remote driver support system active	Collision Avoidance System AEBs*	Collision Avoidance System AEBs*	Vehicle fully automated	Vehicle fully automated	Vehicle fully automated
Responsibility	On-site Operator	Remote Operator	Automated Vehicle	Automated Vehicle	Automated Vehicle
Operator location	< 6 m	On the territory	On the territory	On the territory	On the territory
Speed limitation	6 km/h	6 km/h	Road limitation	Road limitation	Road limitation
Operational safety criteria (MRM trigger)	Remote controller communication	Video latency Driving data command latency	ADS operational Internet connection	ADS operational Internet connection	ADS operational Internet connection
Typical situation	Tele Driving not possible - Bad Internet connection - Bad visibility through camera	Teleassistance L1 not possible - ADS not able to drive autonomously - Complex manoeuvre (e.g. put vehicle at the side of the road)	Teleassistance L2 not possible - Vehicle stationary for too long - Improve traffic flow - Priority agreement situation	Vehicle need confirmation or new path - System limitation - Obstruction on the driving path - Vehicle uncertainty - Complex situation	- Automated Vehicle in normal operation - Part of troubleshooting procedure

*AEBs = Advanced Emergency Braking System
*OEDR = Object and Event Detection and Response

Fig-R 3: Taxonomie des niveaux d'opération à distance (Remote Operation Level, ROL)

Comme l'illustre la figure suivante, cette taxonomie établit également une distinction entre les tâches de téléassistance (**Teleassistance**), de téléopération (**Teleoperation**) et de conduite à distance (**Remote Driving**) en fonction des responsabilités de l'opérateur à distance ou du conducteur du véhicule. Les tâches de téléassistance (ROL3-5) et de téléopération (ROL2) sont exécutées par l'opérateur (Remote Operator) au centre de commande à distance (Remote Operation Centre), qui agit en tant qu'assistant distant (**Remote Assistant**) pour la téléassistance ou en tant que conducteur distant (**Remote Driver**) pour la téléopération. Le pilotage manuel (Remote Driving) (ROL1) relève de la responsabilité du conducteur du véhicule (**Vehicle Driver**), qui peut fournir une assistance sur place si nécessaire.

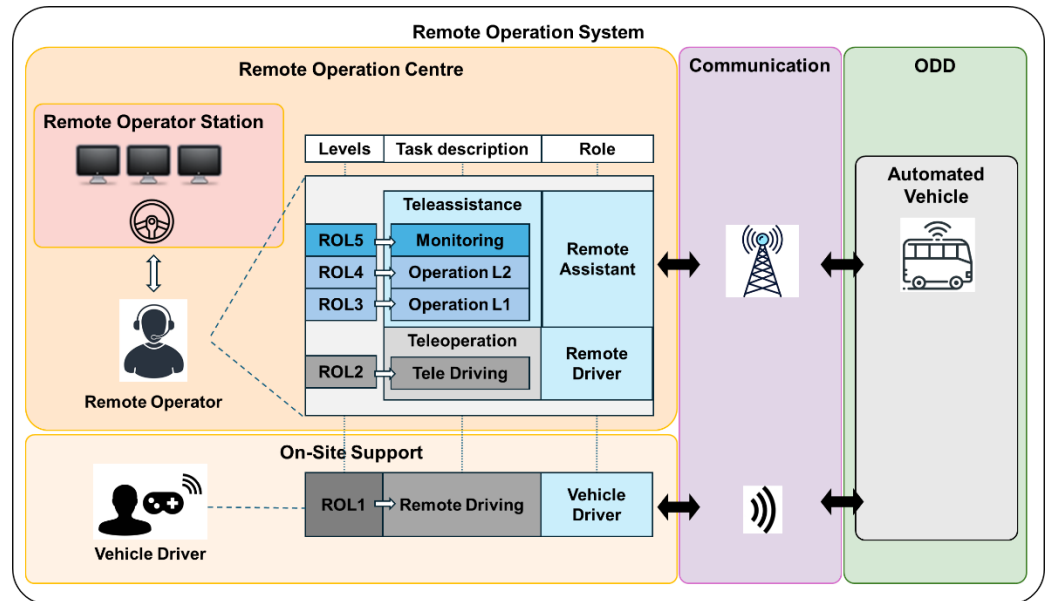


Fig-R 4: Système d'opération à distance (Remote Operation System) avec tâches et rôles

2. Sélection des scénarios

Huit scénarios représentatifs ont été identifiés et analysés, répondant à des défis opérationnels critiques susceptibles de se présenter dans des applications réelles :

- Scénario 1 : Blocage inattendu de la route
- Scénario 2 : Perte de connectivité du réseau ou mauvaise performance du réseau
- Scénario 3 : Localisation imprécise en raison d'un problème du système de localisation ou d'une perte de signal
- Scénario 4 : Dysfonctionnement du capteur optique dû au rayonnement solaire
- Scénario 5 : Le système mondial de navigation par satellite (Global Navigation Satellite System - GNSS) et le compteur kilométrique donnent des résultats ambigus en raison d'une route glissante.
- Scénario 6 : Conditions météorologiques défavorables
- Scénario 7 : Goulot d'étranglement dans un trafic dense

Ces scénarios couvrent une variété de situations complexes, notamment concernant les conditions environnementales, les problèmes de réseau et les dysfonctionnements du système, offrant ainsi un cadre structuré pour l'évaluation des capacités d'un Remote Operation System.

3. Développement des exigences

À partir d'une base de données initiale d'environ 1 000 exigences fournies par les partenaires du projet LOXO, ROSAS/SwissMoves et BFH, l'équipe de recherche a systématiquement distillé un ensemble de 247 exigences classées par ordre de priorité et réparties en trois groupes principaux :

- **Exigences basées sur les ROL (25)** : Répondre aux besoins et fonctionnalités spécifiques de chaque ROL, en veillant à l'alignement sur les objectifs opérationnels et les normes de sécurité
- **Exigences basées sur des scénarios (29)** : Relever les défis posés par divers contextes opérationnels réels, tels que des conditions météorologiques défavorables, des dysfonctionnements des capteurs et des perturbations du réseau
- **Exigences en matière de cybersécurité (193)** : Fournir une protection complète contre les menaces internes et externes, en préservant les canaux de communication, l'intégrité des systèmes et la sécurité opérationnelle

Ce cadre d'exigences affiné constitue une base solide pour les processus de développement de systèmes et d'approbation réglementaire.

4. Validation et tests

Pour évaluer la faisabilité et la fiabilité des exigences du Remote Operation System proposées, le projet de recherche a utilisé une approche de validation à multiples facettes. Celle-ci comprenait une validation basée sur des scénarios, des tests sur site des capacités critiques du système et des évaluations rigoureuses de la cybersécurité.

a) Validation par scénario

L'équipe de recherche a conçu huit scénarios représentatifs pour refléter les défis du monde réel, tels que les perturbations du réseau, les conditions météorologiques défavorables et les dysfonctionnements des capteurs. Ces scénarios ont permis d'évaluer l'applicabilité du système et de tester les exigences proposées dans diverses conditions opérationnelles.

b) Tests sur site

Trois catégories distinctes de tests sur site ont été réalisées avec les véhicules LOXO Alpha et BFH Smartshuttle sur la piste d'essai du DTC. Chaque essai a permis d'évaluer des aspects critiques de la performance du système dans diverses conditions :

- Les **tests de slalom** ont permis d'examiner la manœuvrabilité du système à différentes latences. Un total de 16 essais, effectués à une vitesse maximale de 6 km/h, a révélé que les véhicules, sous le contrôle de l'opérateur, respectaient avec précision la trajectoire désignée à des temps de latence allant jusqu'à 850 ms, démontrant ainsi la stabilité des performances à ces niveaux. À une latence plus élevée de 1 250 ms, une certaine baisse de précision a été observée, mais l'effet n'était pas statistiquement significatif, ce qui met en évidence la résilience du système pour les opérations ROL2 à faible vitesse. Les opérateurs ont décrit les scénarios à forte latence comme étant difficiles mais gérables avec une formation adéquate.

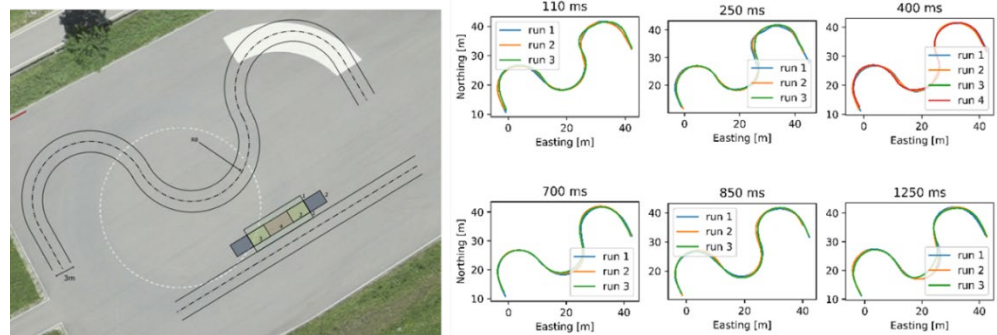


Fig-R 5: Vue aérienne de la piste d'essai de slalom au DTC avec les données de localisation des tests de slalom.

Les **tests de stationnement** ont permis d'évaluer la précision et la réactivité du système lors des manœuvres à faible vitesse. Sur 33 essais, les opérateurs n'ont signalé aucun effet de latence notable, même à 1 000 ms. Les séquences de parcage ont été évaluées sur la base du respect des limites désignées, de la précision d'exécution et de l'évitement des obstacles. Bien que les manœuvres de stationnement soient intrinsèquement difficiles, la latence n'a pas été identifiée comme un facteur limitant, ce qui indique que le système est capable de gérer ces tâches efficacement.

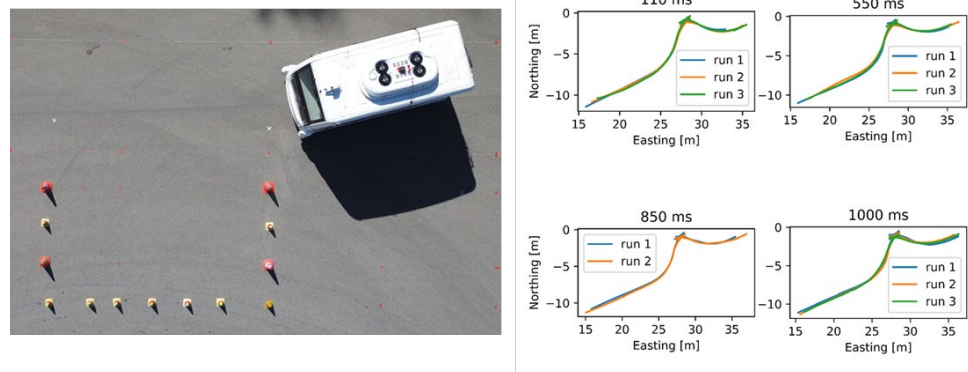


Fig-R 6: Piste d'essai avec les données de localisation des tests de stationnement

- Dans le **test scénario 8 – Détection d'obstacles "False Positive"**, la capacité du système à réagir à des non-obstacles déclenchant des arrêts d'urgence a été évaluée. Onze essais ont été réalisés avec des objets tels que des branches et des sacs en papier pour simuler des faux positifs. Le système de freinage d'urgence automatisé (AEB) a systématiquement détecté ces objets, provoquant des arrêts d'urgence. Les opérateurs ont réussi à résoudre les scénarios en utilisant **deux approches distinctes : contourner** l'obstacle ou **rouler dessus** à très faible vitesse (<1 km/h). Les résultats ont confirmé la pertinence de ce scénario, démontrant que le système pouvait gérer de manière fiable de tels événements dans le respect des exigences définies.



Fig-R 7: Scénario 8 - Détection d'obstacle « False positive » - solution contournant avec ROL2

c) Validation de la cybersécurité

Pour garantir une protection solide contre les menaces internes et externes, un sous-ensemble de 80 des 193 exigences de cybersécurité définies a été rigoureusement testé. Les tests de pénétration sur le véhicule LOXO Alpha ont validé la conformité avec des normes telles que ISO/IEC 27001:2022 et le règlement n° 155 des Nations unies. Bien que les résultats de ces tests soient restés confidentiels, ils ont mis en évidence la capacité du système à répondre à des critères de cybersécurité rigoureux.

d) Principaux résultats

Les principaux résultats de la phase de validation de ce projet sont les suivantes :

- **Tolérance de latence** : Des temps de latence allant jusqu'à 850 ms n'ont pas eu d'impact négatif sur la manœuvrabilité aux faibles vitesses typiques de ROL2 (max. 6 km/h). Des vitesses plus élevées et d'autres scénarios complexes nécessitent un examen plus approfondi pour déterminer les impacts potentiels de la latence
- **Pertinence du scénario** : Le scénario de détection d'obstacles "False Positive" a été confirmé comme étant un problème critique et réel qui peut être résolu avec la conception actuelle du système
- **Défis pour les opérateurs** : Les réactions des opérateurs ont mis en évidence l'importance de la formation pour gérer efficacement les conditions de latence élevée et les manœuvres difficiles

Recommandations

Ce projet de recherche représente une étape importante dans l'avancement des Remote Operation Systems pour les véhicules automobiles, en relevant des défis urgents et en jetant les bases de futures opportunités dans le domaine de la téléassistance et de la téléopération. Grâce à l'élaboration et à la validation d'une taxonomie de niveaux d'opération à distance (Remote Operation Level - ROL) et à la définition d'exigences minimales, le projet établit un cadre solide pour garantir la sécurité, la fiabilité et l'efficacité des opérations à distance. L'approche innovante de validation basée sur des scénarios a démontré la pertinence pratique des exigences et a mis en évidence la résilience de ces systèmes, en particulier à faible vitesse et avec des temps de latence modérés.

Les principaux résultats des essais expérimentaux, tels que la robustesse du système face à des latences allant jusqu'à 850 ms (où la vitesse maximale du véhicule contrôlé par téléopération en ROL2 ne doit pas dépasser 6 km/h) et la gestion réussie de scénarios complexes tels que la détection d'obstacles "False Positifs", confirment que les Remote Operation Systems sont prêts à être déployés sur le terrain. Dans le même temps, le projet met en évidence des domaines nécessitant une exploration plus poussée, en particulier les performances du système dans des conditions de fonctionnement variées, dans des environnements urbains et dans des conditions extrêmes. Les résultats de cette recherche soulignent l'importance cruciale de mesures de sécurité robustes, de l'adaptabilité du système et du développement continu des Remote Operation Systems. Ces exigences minimales servent non seulement de repères techniques et opérationnels, mais constituent également la base permettant aux systèmes d'obtenir une approbation réglementaire formelle. Le respect de ces exigences est essentiel pour l'autorisation, du fonctionnement et le déploiement à grande échelle de ces systèmes.

Pour tirer parti de ces résultats, les recommandations suivantes s'inscrivent dans le cadre des priorités définies dans le présent rapport :

1. La sécurité comme principe fondamental

La sécurité reste le pilier central d'un Remote Operation System. Toutes les avancées technologiques, les mises à jour réglementaires et les stratégies opérationnelles doivent donner la priorité à la protection de tous les usagers de la route et des occupants des véhicules. Cela implique de garantir des liens de communication stables, des capacités de prise de décision en temps réel et des mesures de redondance pour gérer les défaillances inattendues.

2. Affinement et élargissement des définitions des scénarios

Il est essentiel d'actualiser en permanence les définitions des scénarios en tenant compte des enseignements tirés des applications dans le monde réel. En plus d'affiner les scénarios existants, il est crucial d'en développer de nouveaux qui répondent aux défis opérationnels émergents, tels que l'augmentation de la vitesse des véhicules, les environnements urbains complexes et les conditions météorologiques défavorables. Cette approche permet de s'assurer que les scénarios

restent complets et conformes à l'évolution des exigences des Remote Operation Systems.

3. Développement technologique et adaptation aux nouvelles normes

Les technologies d'exploitation à distance et de communication évoluant, il est essentiel de procéder à des examens et à des mises à jour périodiques des exigences définies. Ces mises à jour devraient intégrer les progrès réalisés dans des domaines tels que la connectivité 5G, les stratégies de flux de données adaptatives et l'allocation dynamique des ressources. Ces innovations optimiseront l'utilisation de la bande passante de la liaison montante, favoriseront l'évolutivité pour les opérations de flotte à grande échelle et amélioreront la fiabilité opérationnelle. Le retour d'expérience des applications réelles et l'alignement sur les réglementations internationales émergentes permettront d'affiner ces exigences.

3. Optimisations pour la téléopération (ROL2)

Des améliorations spécifiques pour les opérations ROL2 sont nécessaires pour garantir une intervention transparente à faible vitesse (≤ 6 km/h). La recherche devrait se concentrer sur l'amélioration des interfaces pour les opérateurs à distance, l'étude plus détaillée des effets de la latence (par exemple, les effets des latences fluctuantes), l'amélioration de la réactivité du système pour répondre aux besoins des scénarios de contrôle direct, et la prise en compte des exigences ergonomiques, psychologiques et cognitives des opérateurs pour la téléopération et la téléassistance.

4. Révision périodique et développement ultérieur

La nature dynamique de la mobilité automatisée nécessite des réévaluations régulières des normes techniques et des cadres opérationnels. Ces examens périodiques devraient permettre de relever de nouveaux défis, d'intégrer les percées technologiques et d'évaluer les implications des changements réglementaires sur la conception et le déploiement des systèmes.

5. Formation et certification des opérateurs

Il est essentiel de mettre en place des programmes de formation complets pour les opérateurs. Ces programmes doivent comprendre des simulations pratiques de scénarios d'urgence, une connaissance approfondie des systèmes du véhicule et une compréhension claire des règles de circulation applicables. Les processus de certification doivent garantir que les opérateurs répondent aux normes les plus élevées en matière de compétence et de préparation.

6. Alignement sur les normes internationales

L'harmonisation des exigences nationales avec les normes internationales, telles que le règlement n° 46 des Nations unies et la norme ISO 16505:2019, est essentielle pour garantir l'interopérabilité et l'applicabilité à l'échelle mondiale. Des mises à jour régulières pour s'aligner sur les progrès des systèmes de caméra-moniteur, les repères de latence et les réglementations en matière de sécurité favoriseront une mise en œuvre cohérente dans les différentes juridictions.

L'avenir et les applications pratiques

Les résultats du projet et l'expertise développée positionnent le consortium comme une ressource précieuse pour soutenir la mise en œuvre de l'ordonnance OCA/VAF, introduite par le biais d'un processus de consultation le 18 octobre 2023 [3] et adoptée par le Conseil fédéral le 13 décembre 2024 [4]. Ce projet de recherche aborde directement les dispositions clés décrites dans le chapitre 5 de l'ordonnance OCA/VAF [5], garantissant l'état de préparation opérationnelle et la sécurité des véhicules sans conducteur. La terminologie et la taxonomie développées dans le cadre du projet, en particulier la compréhension structurée des niveaux d'opération à distance (ROL), sont des outils essentiels pour clarifier les responsabilités et permettre la conformité avec le nouveau cadre réglementaire.

En tirant parti de sa solide base de connaissances pour définir et valider les exigences minimales des systèmes d'opération à distance, le consortium pourrait accompagner les autorités fédérales dans l'évaluation pour l'autorisation et l'exploitation de tels systèmes. Il s'agit notamment d'effectuer des évaluations techniques, de soutenir le processus d'autorisation et de fournir des services de formation et de consultation. Ces efforts comblent le fossé entre les exigences légales et la mise en œuvre pratique, garantissant l'intégration sûre et efficace des véhicules sans conducteur (AVs) dans le réseau routier public. [12] [13]. Ce rôle est particulièrement important compte tenu des défis que représente l'intégration ses systèmes d'opération à distance (Remote Operation System) dans des paysages technologiques et réglementaires en évolution rapide. Les exigences définies dans le projet représentent un instantané des capacités actuelles et nécessiteront des mises à jour périodiques pour tenir compte des progrès, des changements dans les normes internationales et de l'évolution de la réglementation.

En tant qu'intermédiaires entre la conduite manuelle et la conduite entièrement automatisée, la téléopération et la téléassistance constituent des technologies essentielles pour assurer la transition vers la mobilité automatisée. Ces systèmes permettent de combler les lacunes opérationnelles dans le déploiement et l'utilisation des véhicules sans conducteurs (AVs), en particulier dans les scénarios où l'automatisation complète n'est pas encore possible. En outre, le consortium pourrait favoriser la collaboration entre les autorités publiques, les acteurs de l'industrie et les institutions de recherche, en promouvant l'intégration sûre et efficace des véhicules sans conducteurs dans l'écosystème des transports en Suisse.

Summary

Problem description

The global transition towards automated mobility has led to significant advancements in automated vehicle (AV) technologies. Pilot projects, internationally but also in Switzerland, have demonstrated the potential of AVs in diverse applications such as last-mile public transport connections and goods delivery. In Switzerland, organizations such as **SAAM** (Swiss Association for Autonomous Mobility) [1] and **SwissMoves** [2] play a central role in promoting collaboration between industry, academia, and public authorities. These organizations not only support the development and implementation of cutting-edge projects but also serve as key platforms for disseminating knowledge and fostering innovation in the field of automated and connected mobility.

In Switzerland, at the time of writing this report in 2024, road traffic regulations mandate the presence of a qualified operator on board AVs to assume control in critical situations. This requirement limits the economic viability of AV operations. The Swiss Federal Roads Office (FEDRO) initiated a consultation process on 18 October 2023 to develop a new legal framework [3], which concluded with the Federal Council's adoption of the “Ordonnance sur la conduite automatisée” (**OCA**) / “Verordnung über das automatisierte Fahren” (**VAF**) on 13 December 2024 [4]. This ordinance [5], set to come into force on 1 March 2025, establishes comprehensive operational requirements for driverless AVs. According to this regulation, the driverless AVs must be monitored by an Operator, who can intervene remotely when the vehicle encounters a situation it cannot resolve autonomously.

The deployment of driverless AVs, particularly for last-mile public transport operations and goods transport, is seen as a viable solution to address current operational challenges. Remote Operation Systems enable economic feasibility by facilitating remote interventions, bridging the gap where full automation is not yet achievable.

The technical capabilities for Remote Operation Systems have progressed significantly. Modern systems now integrate advanced sensors, cameras, and data communication technologies, enabling real-time monitoring and control. However, to establish a reliable approval process for these Remote Operation Systems, comprehensive and robust requirements must be defined, encompassing traffic safety, IT security, data protection, cybersecurity resilience, and operator training. The research project commissioned by FEDRO addresses these challenges by defining and validating minimum requirements for Remote Operation Systems, building on national and international research. Leveraging expertise gained from Switzerland's first Teleoperation centre [6] [7] and other pilot projects, this interdisciplinary effort ensures alignment with evolving technological and regulatory landscapes while

meeting high safety and reliability standards. A particular focus was placed on ensuring cybersecurity resilience through regular testing, monitoring, and alignment with international standards.

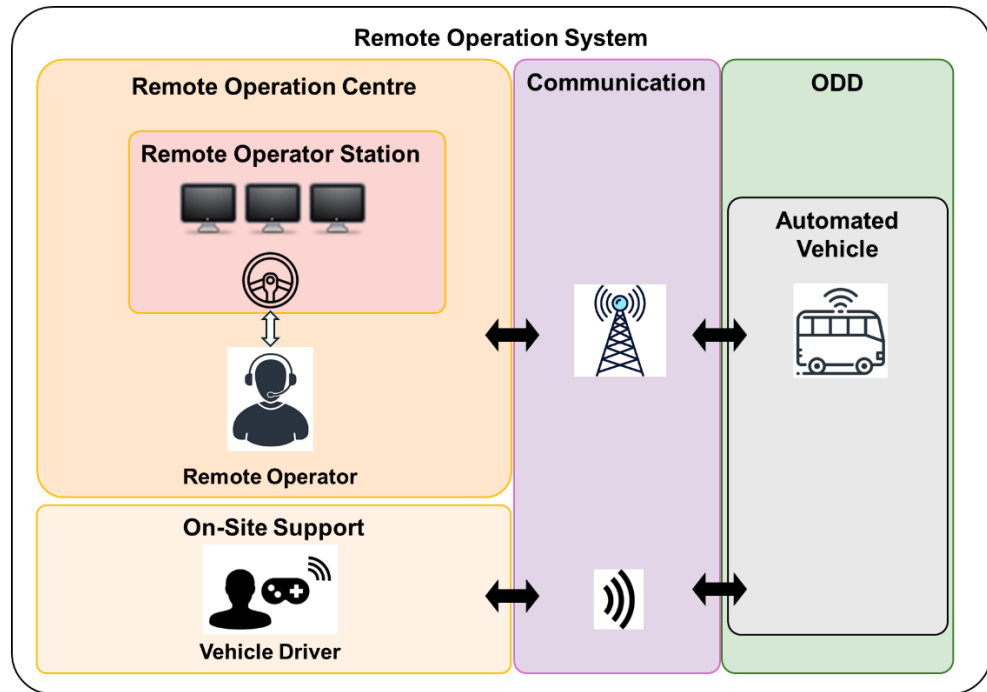


Fig-S 1: Overview of the Remote Operation Systems

Objectives

The research project addresses the key challenge of ensuring that Remote Operation Systems meet high safety and reliability standards, while also aiming to advance technological and regulatory advancements. To achieve this, the project pursued two primary objectives:

1. Define minimum requirements with regard to traffic safety, traffic flow and IT security for a Remote Operation System:

The project aimed to establish a comprehensive set of safety, cybersecurity, and operational requirements for Remote Operation Systems. These requirements serve as a foundation for the evaluation, approval and operation of such systems. Key aspects include:

- **Operational Design Domain (ODD):** Consideration of infrastructure, weather conditions, and interactions with other road users
- **Automated Vehicle (AV):** Specification of perception technologies, sensors, and actuators critical for reliable operation
- **Communication:** Focus on IT security, latency management, redundancy, and reliability to ensure robust data exchange
- **Remote Operator Station:** Development of advanced visualisation and audio technologies to enhance operator interaction with AVs
- **Remote Operator:** Definition of training standards and key competencies required for effective and safe system operation

2. Provide the basis to better understand the limits of Remote Operation systems and to derive requirements for their evaluation and approval

To support the integration and regulation of Remote Operation Systems, the project focused on identifying their operational boundaries and deriving criteria for their evaluation and approval. This involved:

- **Aligning requirements** with international standards and national regulatory frameworks to ensure consistency and scalability
- **Validating requirements** through a combination of theoretical analyses, experimental testing, and scenario evaluations, ensuring their applicability in real-world contexts

Note that the project specifically targets AVs with driving automation Level 4 or 5 (ISO/SAE PAS 22736, 2021), as these levels provide the necessary baseline for Remote Operation Systems. While these vehicles are capable of handling most driving tasks automatically, they rely on support from a Remote Operator to ensure safe and reliable operation in scenarios where full automation is not yet feasible.

Methodology

To ensure a robust foundation for Remote Operation Systems, the project adopted a systematic and multidisciplinary approach, integrating real-world testing, stakeholder consultations, and compliance with established standards. The methodology comprised the following key elements:

1. Scenario development and definition of a Taxonomy

Eight representative scenarios were created to simulate real-world challenges, such as network disruptions, adverse weather, and urban traffic complexities. These scenarios provided a structured framework for evaluating the Remote Operation System's performance across varied operational conditions and served as a foundation for defining the Remote Operation Levels (ROLs). Building on the DriveU.auto framework, the project developed a comprehensive Taxonomy of five Remote Operation Levels (ROL₁–ROL₅).

2. Requirements Definition

As part of the methodology, the project team systematically grouped the defined requirements into three main categories:

- **ROL-Based Requirements:** Addressing the specific needs and roles of Remote Operators at different Remote Operation Levels
- **Scenario-Based Requirements:** Focused on addressing operational challenges under diverse real-world conditions
- **Cybersecurity Requirements:** Ensuring robust protection against external and internal threats, covering data integrity, network reliability, and system resilience

3. Validation Approaches

Three complementary validation methods were employed to ensure the reliability and applicability of the defined requirements:

- **Alignment with international standards and regulatory frameworks:** Ensuring alignment with international regulations such as UNECE, ISO standards, and the new OCA/VAF ordinance of Switzerland
- **Scenario-based validation:** Testing requirements against the selected scenarios to confirm their relevance and applicability
- **Theoretical and experimental testing:** Assessing impacts of network latency, obstacle detection capabilities, and other critical factors through on-site test drives and simulations

4. Cybersecurity Validation

Cybersecurity was a central focus, with 193 specific requirements defined to protect the Remote Operation System. These requirements addressed threats to the AV, communication channels, and Remote Operation Station. Validation activities included a rigorous penetration testing campaign, ensuring that the defined cybersecurity measures can be tested both practically and effectively.

5. Stakeholder Engagement

Workshops and interviews with industry experts, regulators, and academic researchers provided invaluable insights. This collaboration enriched the project’s findings, ensuring their relevance to real-world challenges and alignment with the needs of future Remote Operation Systems.

Legal Frameworks and Standards

The regulatory landscape for automated and remotely operated vehicles is complex (see figure below), with evolving international and national standards shaping their integration. Two pivotal international legal acts, the **Geneva Convention on Road Traffic** (1949) [8] and the **Vienna Convention on Road Traffic** (1968, amended 2016/2021) [9], serve as foundational treaties, addressing driver responsibilities and enabling remote operations under specific conditions. These conventions are complemented by **UNECE regulations**, such as **Regulation No. 155 Cybersecurity** [10] and **Regulation No. 156 Software Updates** [11], which provide detailed technical requirements to ensure system safety and interoperability.

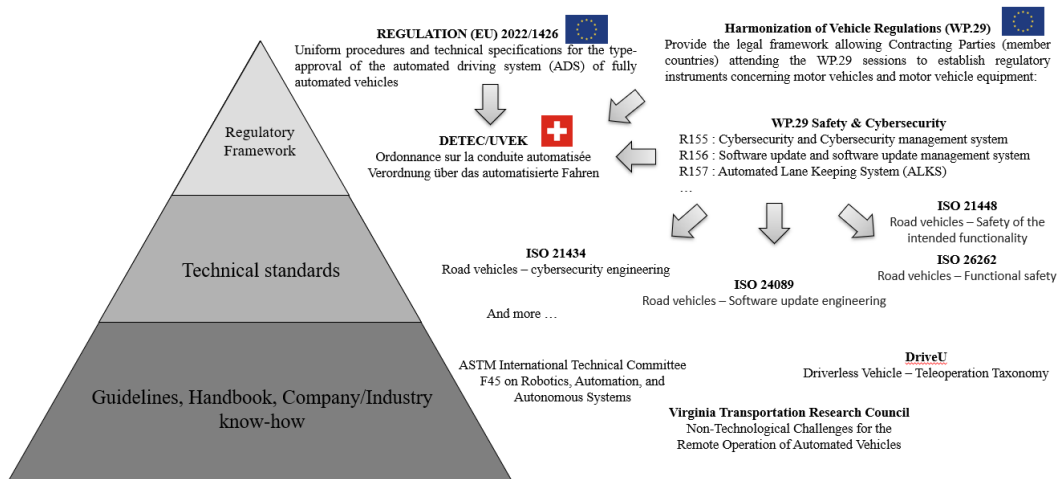


Fig-S 2: Overview of regulations, standards and guidelines

In **Switzerland**, the Federal Council launched a consultation process on October 18, 2023, to introduce the **OCA/VAF ordinance**. The ordinance was adopted by the Federal Council on 13 December 2024 and will come into force on 1 March 2025 [4]. The following key provisions are designed to establish comprehensive operational requirements for driverless vehicles with an automation system:

- **Art. 33:** Before daily operation, driverless vehicles must undergo a departure check which involves a manual driving manoeuvre
- **Art. 34:** Responsibilities for operators, including monitoring vehicle performance, managing automation systems, and initiating safety measures during critical situations. Operators must be based in Switzerland and must have completed required trainings
- **Art. 35:** Specifies requirements for the manual operation of driverless vehicles, emphasizing that individuals manually operating the vehicle are considered drivers under road traffic regulations but are not classified as Remote Operators. Transitions between automated and manual modes are only allowed when the vehicle is stationary
- **Art. 36:** Requirements for the operator or the person who manually operates the driverless vehicle, including driving aptitude, driving competence, driving licence, training and further training on the driverless vehicle
- **Art. 37:** Guidelines for the training of operators, in particular with regard to the technical functioning of the vehicle and the automation systems
- **Art. 38:** Requires vehicle owners to ensure that vehicles are only operated by qualified personnel and that technical maintenance and communication infrastructures are in place
- **Art. 41:** Requires driverless vehicles to have a driving mode recorder that logs key events, including the activation and deactivation of the automation system, risk-reduction manoeuvres, communication between the vehicle and the operator, and interruptions in the communication link
- **Art. 42:** In the case of driverless vehicles, the automation system must recognise and comply with the limits of the approved area of use
- **Art. 43:** Detailed requirements for obtaining operational authorisation, including documentation of remote intervention capabilities and communication reliability under defined conditions of use
- **Art. 50:** FEDRO will evaluate the effects of the ordinance, which may influence future adjustments and research requirements

These articles emphasize the importance of rigorous operator training, robust system maintenance, and effective risk-reduction procedures. By incorporating these provisions, the OCA/VAF ordinance aims to ensure the safe integration of driverless vehicles into public road networks while also addressing the unique challenges posed by such technologies.

Results

The research project delivered important results that define the foundations for Remote Operation Systems, emphasizing a clear Taxonomy, comprehensive requirements, and a scenario selection for testing and validation.

1. Terminology and Taxonomy

A comprehensive Taxonomy for **Remote Operation Levels (ROL1–ROL5)** was developed, clearly defining the roles and responsibilities of Remote Operators and Vehicle Driver across varying degrees of vehicle autonomy and involvement (see figure below). Building on the DriveU.auto framework, this taxonomy was refined and adapted to address the specific needs identified in the developed scenarios. Its simplicity and flexibility make it a foundational element for both the requirements definition and testing processes in this project.

On-site Remote Driving
without OEDR sensors
 Teleoperation
with OEDR sensors
 ← Teleassistance →

Remote Operation Level	ROL 1	ROL 2	ROL 3	ROL 4	ROL 5
Designation	Remote Controller Driving	Tele Driving	Teleassistance Operation L1	Teleassistance Operation L2	Monitoring
Task	Full control of the vehicle Act like a normal driver Communication	Full control on the vehicle Act like a normal driver Communication	Path drawing Speed control Lights or other control Communication	Path drawing Path confirmation Communication	Supervision Communication
DDT responsibility of operator	Full	Full	Speed application	None	None
OEDR responsibility of operator	Full	None	None	None	None
Remote driver support system active	Collision Avoidance System AEBS*	Collision Avoidance System AEBS*	Vehicle fully automated	Vehicle fully automated	Vehicle fully automated
Responsibility	On-site Operator	Remote Operator	Automated Vehicle	Automated Vehicle	Automated Vehicle
Operator location	< 6 m	On the territory	On the territory	On the territory	On the territory
Speed limitation	6 km/h	6 km/h	Road limitation	Road limitation	Road limitation
Operational safety criteria (MRM trigger)	Remote controller communication	Video latency Driving data command latency	ADS operational Internet connection	ADS operational Internet connection	ADS operational Internet connection
Typical situation	Tele Driving not possible - Bad Internet connection - Bad visibility through camera	Teleassistance L1 not possible - ADS not able to drive autonomously - Complex manoeuvre (e.g. put vehicle at the side of the road)	Teleassistance L2 not possible - Vehicle stationary for too long - Improve traffic flow - Priority agreement situation	Vehicle need confirmation or new path - System limitation - Obstruction on the driving path - Vehicle uncertainty - Complex situation	- Automated Vehicle in normal operation - Part of troubleshooting procedure

*AEBS = Advanced Emergency Braking System
*OEDR = Object and Event Detection and Response

Fig-S 3: Taxonomy of Remote Operation Levels (ROLs)

As illustrated in the next figure, this Taxonomy also distinguishes between the tasks of **Teleassistance**, **Teleoperation** and **Remote Driving** in relation to the responsibilities of the Remote Operator or the Vehicle Driver. The tasks of Teleassistance (ROL3–5) and Teleoperation (ROL2) are performed by the **Remote Operator** in the Remote Operation Centre, acting as the **Remote Assistant** for Teleassistance or the **Remote Driver** for Teleoperation. Remote Driving (ROL1) falls under the responsibility of the **Vehicle Driver**, who provides on-site support when required.

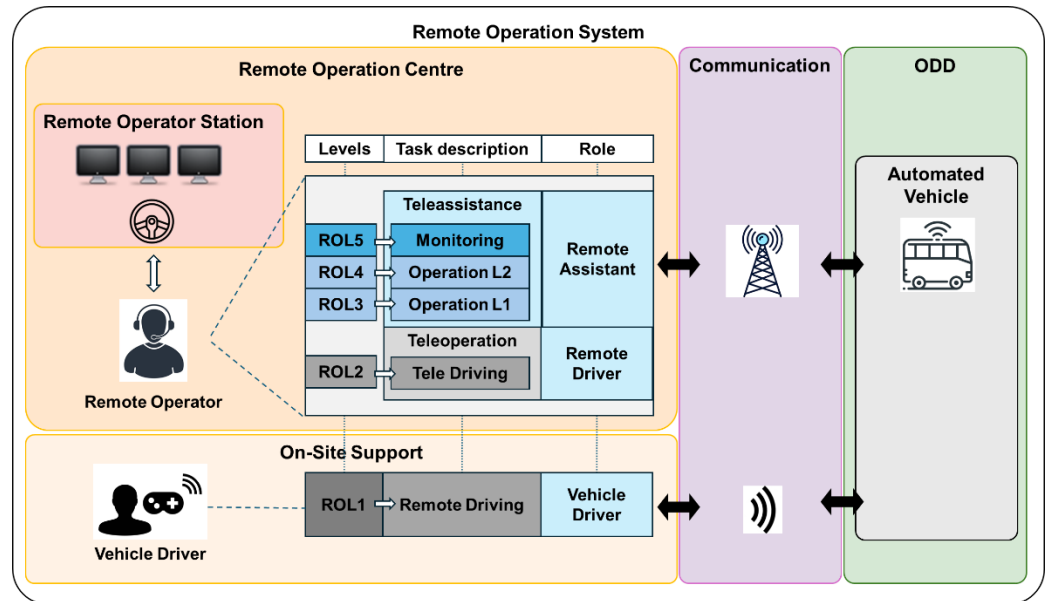


Fig-S 4: Remote Operation System with tasks and roles

2. Scenario Selection

Eight representative scenarios were identified and analysed, addressing critical operational challenges likely to arise in real-world applications:

- Scenario 1: Unexpected road blockage
- Scenario 2: Loss of network connectivity or poor network performance
- Scenario 3: Imprecise location due to location system issue or signal loss
- Scenario 4: Malfunction of optical sensor due to solar radiation
- Scenario 5: Global Navigation Satellite System (GNSS) and odometer give ambiguous results due to slippery road
- Scenario 6: Adverse weather conditions
- Scenario 7: Bottleneck in dense traffic

These scenarios cover a variety of complex situations, including environmental conditions, network issues, and system malfunctions, and provide a structured framework for evaluating the capabilities of Remote Operation Systems.

3. Requirements Development

From an initial database of approximately 1,000 requirements provided by project partners LOXO, ROSAS/SwissMoves and BFH, the research team systematically distilled a prioritized set of 247 requirements, categorized into three main groups:

- **ROL-based requirements (25):** Address specific needs and functionalities for each ROL, ensuring alignment with operational objectives and safety standards
- **Scenario-based requirements (29):** Tackle challenges presented by diverse real-world operational contexts, such as adverse weather conditions, sensor malfunctions, and network disruptions
- **Cybersecurity requirements (193):** Provide comprehensive protection against internal and external threats, safeguarding communication channels, system integrity, and operational safety

This refined requirement framework forms a robust foundation for both system development and regulatory approval processes.

4. Validation and Testing

To evaluate the practicality and reliability of the proposed Remote Operation System requirements, the research project employed a multifaceted validation approach. This included scenario-based validation, on-site testing of critical system capabilities, and rigorous cybersecurity assessments.

a) Scenario-Based Validation

The research team designed eight representative scenarios to reflect real-world challenges, such as network disruptions, adverse weather, and sensor malfunctions. These scenarios were instrumental in assessing the system's applicability and testing the proposed requirements against diverse operational conditions.

b) On-Site testing

Three distinct on-site test categories were performed using the LOXO Alpha and BFH Smartshuttle vehicles on the DTC test track. Each test evaluated critical aspects of system performance under various conditions:

- **Slalom Tests** examined the system’s manoeuvrability at varying latencies. A total of 16 test runs, conducted at a maximum speed of 6 km/h, revealed that the vehicles, under control of the Teleoperator, maintained accurate adherence to the designated path at latencies up to 850 ms, demonstrating stable performance at these levels. At a higher latency of 1250 ms, some decline in precision was observed, but the effect was not statistically significant, highlighting the system’s resilience for ROL2 operations at low speeds. Remote Operators described the high-latency scenarios as challenging but manageable with adequate training.

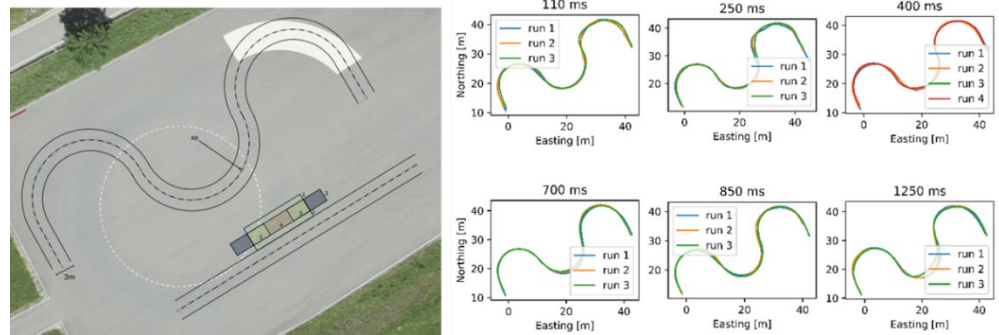


Fig-S 5: Aerial view of slalom test track at DTC with location data of slalom tests

- **Parking Tests** evaluated the precision and responsiveness of the system during low-speed manoeuvres. Across 33 test runs, the Remote Operators reported no noticeable latency effects, even at 1000 ms. The parking sequences were assessed based on adherence to designated boundaries, execution precision, and obstacle avoidance. While parking manoeuvres were inherently challenging, latency was not identified as a limiting factor, indicating the system’s capability to handle these tasks effectively.

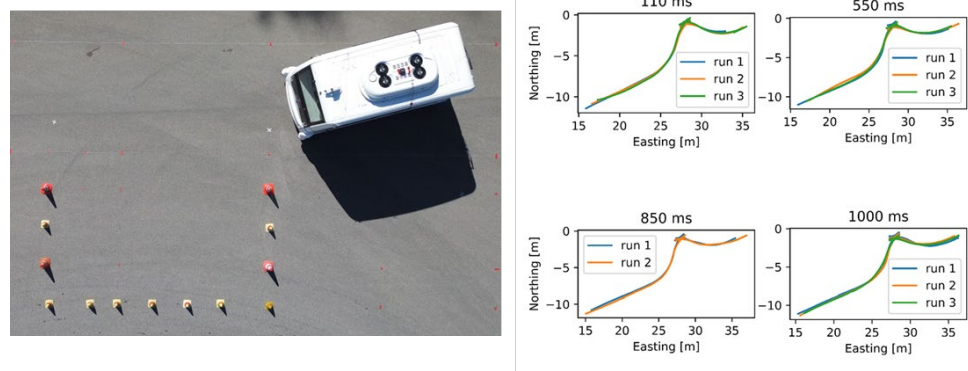


Fig-S 6: Parking test track with location data of parking tests

- **In the Scenario 8 – False Positive Obstacle Detection tests**, the system’s ability to respond to non-obstacles triggering emergency stops was evaluated. Eleven test runs were conducted using objects like branches and paper bags to simulate false positives. The Automated Emergency Braking (AEB) system consistently detected these objects, prompting emergency stops. Remote Operators successfully resolved the scenarios using **two distinct approaches: bypassing** the obstacle and **driving over** it at very low speeds (<1 km/h). The results confirmed the relevance of this scenario, demonstrating that the system could reliably handle such events within the defined requirements.



Fig-S 7: Scenario 8 - False positive obstacle detection - solution bypassing ROL2

c) Cybersecurity Validation

To ensure robust protection against internal and external threats, a subset of 80 out of 193 defined cybersecurity requirements were rigorously tested. Penetration tests on the LOXO Alpha vehicle validated compliance with standards like ISO/IEC 27001:2022 and UN Regulation No. 155. Although sensitive test results were confidential, they underscored the system’s capability to meet stringent cybersecurity benchmarks.

d) Key findings

The key findings of the validation phase of this project are:

- **Latency Tolerance:** Latencies up to 850 ms were found to have no detrimental impact on manoeuvrability at ROL2’s typical low speeds (max 6km/h). Higher speeds and other complex scenarios require further investigation to determine potential latency impacts
- **Scenario Relevance:** The scenario "False Positive" obstacle detection was confirmed as a critical, real-world issue solvable with the current system design
- **Operator Challenges:** Feedback from Remote Operators highlighted the importance of training to handle high-latency conditions and challenging manoeuvres effectively

Recommendations

This research project represents a significant milestone in advancing Remote Operation Systems with AVs, addressing pressing challenges and laying the foundation for future opportunities in Teleassistance and Teleoperation. Through the development and validation of a comprehensive taxonomy for Remote Operation Levels (ROLs) and the definition of minimum requirements, the project establishes a robust framework for ensuring safety, reliability, and efficiency in remote operations. The innovative scenario-based validation approach demonstrated the practical relevance of the requirements and highlighted the resilience of these systems, particularly at low speeds and under moderate latencies.

Key findings from the experimental testing, such as the robustness of the system to latencies up to 850 ms (where the maximum speed of the vehicle controlled by Teleoperation in ROL2 shall not exceed 6 km/h) and the successful handling of complex scenarios like "False Positive Obstacle Detection", confirm the readiness of Remote Operation Systems for operational deployment. At the same time, the project underscores areas requiring further exploration, particularly system performance under varied operating conditions, urban environments, and extreme conditions. The findings of this research emphasize the critical importance of robust safety measures, system adaptability, and ongoing development in Remote Operation Systems. These minimum requirements not only serve as technical and operational benchmarks but also provide the foundation for enabling systems to obtain formal regulatory approval. Ensuring compliance with these requirements is essential for the successful authorisation, operation and widespread deployment of such systems.

To build on these results, the following recommendations align with the priorities outlined in this report:

1. Focus on Safety as a fundamental principle

Safety remains the central pillar of Remote Operation Systems. All technological advancements, regulatory updates, and operational strategies should prioritize the protection of all road users and vehicle occupants. This includes ensuring stable communication links, real-time decision-making capabilities, and redundancy measures to manage unexpected failures.

2. Refinement and expansion of Scenario definitions

Continuous updates to scenario definitions are essential, incorporating insights gained from real-world applications. In addition to refining existing scenarios, it is crucial to develop new ones that address emerging operational challenges, such as higher vehicle speeds, complex urban environments, and adverse weather conditions. This approach ensures the scenarios remain comprehensive and aligned with the evolving demands of Remote Operation Systems.

3. Technological development and adaptation to new standards

As remote operation and communication technologies evolve, periodic reviews and updates of the defined requirements are essential. These updates should incorporate advancements in areas such as 5G connectivity, adaptive data streaming strategies, and dynamic resource allocation. These innovations will optimise uplink bandwidth usage, support scalability for large-scale fleet operations, and enhance operational reliability. Feedback from real-world applications and alignment with emerging international regulations will further refine these requirements.

4. Refinements for Teleoperation (ROL2)

Specific refinements for ROL2 operations are required to ensure seamless intervention at low speeds (≤ 6 km/h). Research should focus on improving Remote Operator interfaces, studying latency effects in more detail (e.g., effects of varying latencies), and enhancing system responsiveness to meet the needs of direct control scenarios, and addressing the ergonomic, psychological, and cognitive requirements of Remote Operators for both Teleoperation and Teleassistance.

5. Periodic review and further development

The dynamic nature of automated mobility necessitates regular reassessments of both technical standards and operational frameworks. These periodic reviews should address new challenges, integrate technological breakthroughs, and evaluate the implications of regulatory changes on system design and deployment.

6. Training and certification for Remote Operators

Comprehensive training programs for Remote Operators are critical. These programs should include practical simulations of emergency scenarios, in-depth knowledge of vehicle systems, and a clear understanding of applicable traffic regulations. Certification processes must ensure that operators meet the highest standards of competence and readiness.

7. Alignment with international standards

Harmonising national requirements with international standards, such as UN Regulation No. 46 and ISO 16505:2019, is essential to ensure interoperability and global applicability. Regular updates to align with advancements in camera-monitor systems, latency benchmarks, and safety regulations will support consistent implementation across different jurisdictions.

Future and Practical Applications

The project's findings and the expertise developed position the consortium as a valuable resource for supporting the implementation of the OCA/VAF ordinance, introduced through a consultation process on 18 October 2023 [3] and adopted by the Federal Council on 13 December 2024 [4]. This research project directly addresses key provisions outlined in Chapter 5 of the OCA/AFV ordinance [5], ensuring the operational readiness and safety of driverless vehicles. The project's developed terminology and taxonomy, particularly the structured understanding of Remote Operation Levels (ROs), are essential tools for clarifying responsibilities and enabling compliance with the new regulatory framework.

By leveraging its robust foundation of knowledge in defining and validating minimum requirements for Remote Operation Systems, the consortium could assist federal authorities in evaluating the approval and operation of such systems. This includes conducting technical evaluations, supporting the authorisation process, and providing training and consultation services. These efforts bridge the gap between regulatory requirements and practical deployment, ensuring the safe and efficient integration of automated and remotely operated vehicles into public road networks [12] [13]. This role is particularly critical given the challenges of integrating Remote Operation Systems into rapidly evolving technological and regulatory landscapes. The requirements defined in the project represent a snapshot of current capabilities and will necessitate periodic updates to accommodate advancements, changes in international standards, and evolving regulations.

By being an intermediary between manual and fully automated driving, Teleoperation and Teleassistance serve as critical enabling technologies for transitioning to automated mobility. These systems facilitate the closure of operational gaps in the deployment and use of automated vehicles, particularly in scenarios where full automation may not yet be feasible. Furthermore, the consortium could foster collaboration between public authorities, industry stakeholders, and research institutions, promoting the safe and efficient integration of driverless vehicles into Switzerland's transportation ecosystem.

1 Introduction

Ongoing advancements in vehicle automation and remote operation have led to significant changes and new challenges in recent years. This research project focuses on examining the essential requirements and frameworks necessary for the safe and efficient remote operation of Automated Vehicles (AVs) in Switzerland. The following section provides an overview of the current context and situation, laying the foundation for understanding the project's objectives and methodologies.

1.1 Context and Current Situation

The current landscape of AV technology presents considerable potential for transforming the mobility system. Switzerland has established itself as a hub for innovation in the field of automated systems, supported by key organizations like **SAAM** (Swiss Association for Autonomous Mobility) [1] and **SwissMoves** [2], which play a central role in coordinating and promoting activities around automated and connected mobility in Switzerland. These organizations foster collaboration between industry, academia, and public authorities, facilitating the development and implementation of cutting-edge projects. Their platforms provide an overview of ongoing initiatives and serve as knowledge hubs for the advancement of automated systems in Switzerland.

Advances in automated driving technology have led to the development of AVs capable of operating at Level 4 (High Driving Automation, see 7.2) within defined Operational Design Domains (ODDs), such as specific urban areas, highways, or industrial zones. However, full deployment beyond these ODDs, especially at Level 5 (Full Driving Automation, see 7.2), remains a long-term goal due to significant technical and regulatory challenges. Globally, pilot projects for AVs are being conducted in various sectors, including public transportation (Figure 1), goods delivery, and industrial logistics and agricultural automation (Figure 2).



Figure 1: National projects for public transportation [14] [15] [16] [17] [18] [6] [6] [19] [20]

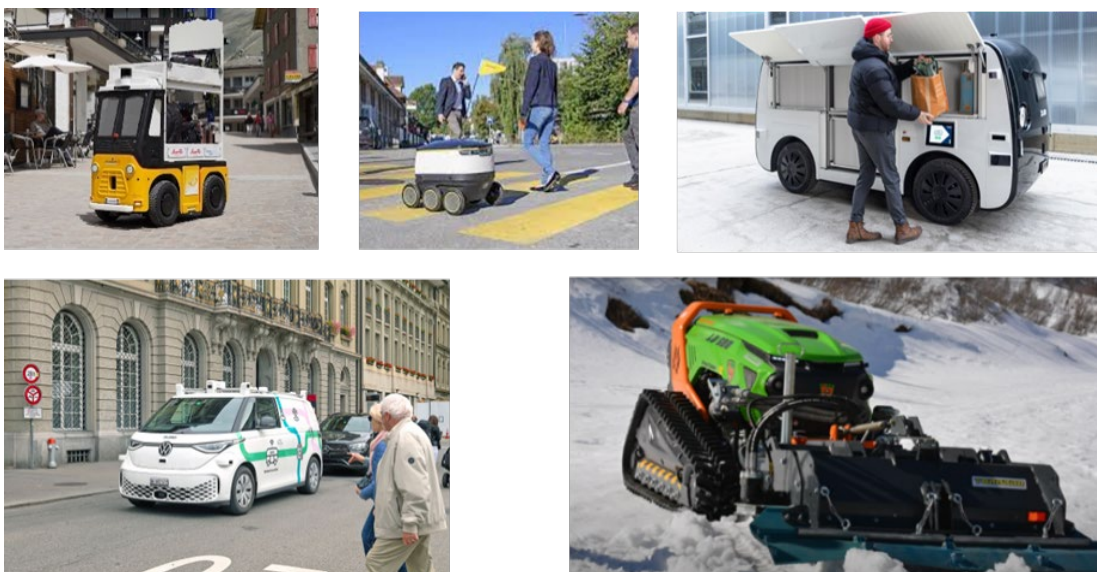


Figure 2: National projects for goods delivery and agricultural automation [21] [22] [23] [24] [25]

In recent years, several pilot projects in the field of automated vehicles have been conducted in Switzerland, focusing on areas such as public transportation (Figure 1), goods delivery and agricultural automation (Figure 2), and the development of business models ([26] [27] [28]). Notables initiatives have also been carried out internationally ([29] [30] [31] [32]). Some of these projects are still ongoing and continue to contribute to the continuous advancement of AV technologies.

Despite these advancements, challenges such as cybersecurity [33], communication latency, sensor reliability, and system redundancy must be addressed to ensure safety and scalability. Sector-specific guidelines like the "Handbuch Cybersecurity für

Betriebe des öffentlichen Verkehrs" [34] provide practical recommendations for addressing cybersecurity challenges and establishing robust cybersecurity measures for critical infrastructure systems, including AVs.

One key challenge is the necessity of removing on-board supervision personnel to make the use of AVs economically viable even as the involvement of qualified personnel in operation of AVs remains essential from both a technological and user trust perspective. A solution can be achieved through the implementation of Remote Operation Centres, where Remote Operators can manage multiple AVs remotely either by Teleassistance or Teleoperation. The importance of such systems has been highlighted in studies, suggesting that truly automated cars may be impossible without the helpful human touch [35]. In Switzerland, a highly successful and innovative Teleoperation project was initiated in 2021 [6], laying the groundwork for further developments in this field. This initial project has since evolved into initiatives like AutoSnow [25], Autoscale [36] and "Dynamic Micro-Hub with LOXO" [24], underscoring Switzerland's leadership in advancing AV Remote Operation technologies.

Technological advancements in automated driving are progressing steadily. AVs classified Level 4, and thus limit operation to areas designated by its ODD, are expected to become available in the medium term [37]. In contrast, Level 5 vehicles, capable of fully automated operation in any environment and without any human driver, are only expected in the long term. Both levels, however, present scenarios where Remote Operation Systems could be utilized to improve vehicle management under certain conditions.

For the approval and integration of these remote-monitored and operated AVs into public transport systems, strict criteria are necessary to ensure traffic safety, traffic flow, IT security, and data protection. This research aims to provide the scientific foundation needed to develop these criteria for the Remote Operation System, which, as illustrated in Figure 3, comprises the Automated Vehicle, the associated ODD, the Communication, the Remote-Operation Centre and the Remote Operator.

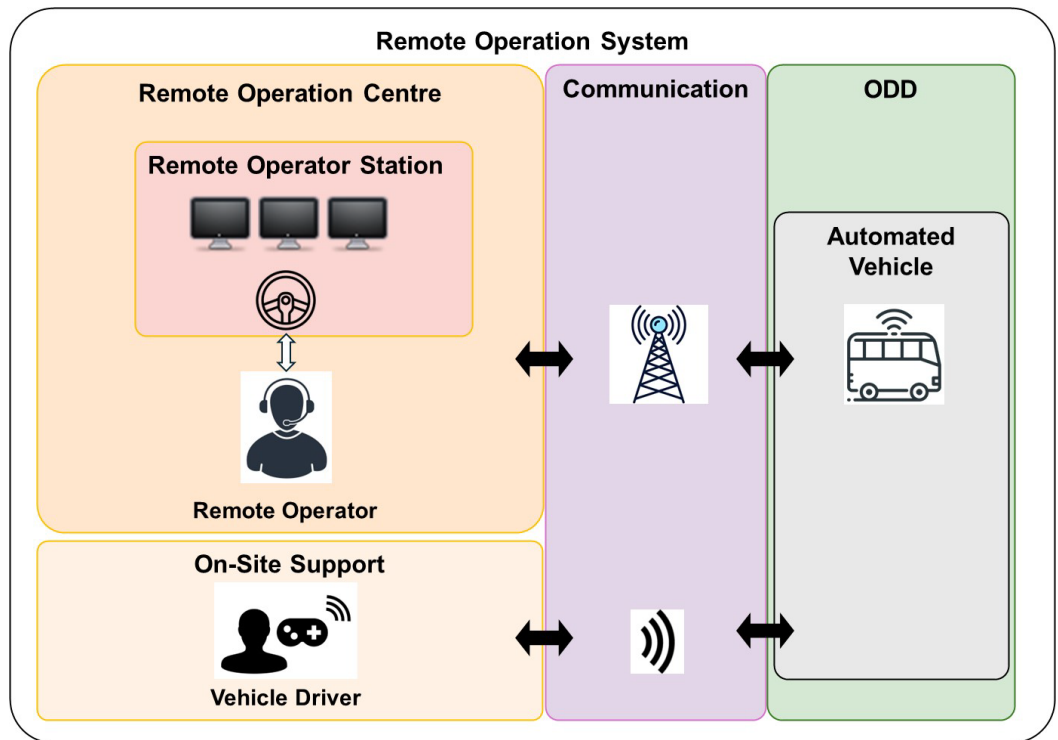


Figure 3: Overview of Remote Operation Systems

In Switzerland, at the time of writing this report in 2024, road traffic regulations mandate the presence of a qualified operator on board AVs to assume control in critical situations. This requirement limits the economic viability of AV operations. The Swiss Federal Roads Office (FEDRO) initiated a consultation process on 18 October 2023 to develop a new legal framework [3], which concluded with the Federal Council's adoption of the “Ordonnance sur la conduite automatisée” (OCA) / “Verordnung über das automatisierte Fahren” (VAF) on 13 December 2024 [4]. This regulation, which is scheduled to take effect on 1 March 2025, establishes comprehensive operational requirements for automated and by operators remotely supervised driverless AVs that enable safe and economical operation of AVs through Remote Operation Systems. These systems help address operational gaps in the deployment and use of AVs, particularly in scenarios where full automation may not yet be feasible.

Defining the scope of requirements to ensure the seamless integration of AVs into the traffic flow, alongside robust measures for IT security and data protection, is crucial for their authorisation and safe operation.

1.2 Motivation and Objectives of the Research Project

The development and deployment of reliable AVs present significant challenges, particularly as these vehicles are not yet capable of handling all possible scenarios independently. Currently, AVs still require human assistance to navigate complex or ambiguous situations. Consequently, and as shown in Figure 4, the concept of Remote Operator assistance for AVs has emerged as an interim step in advancing these technologies.

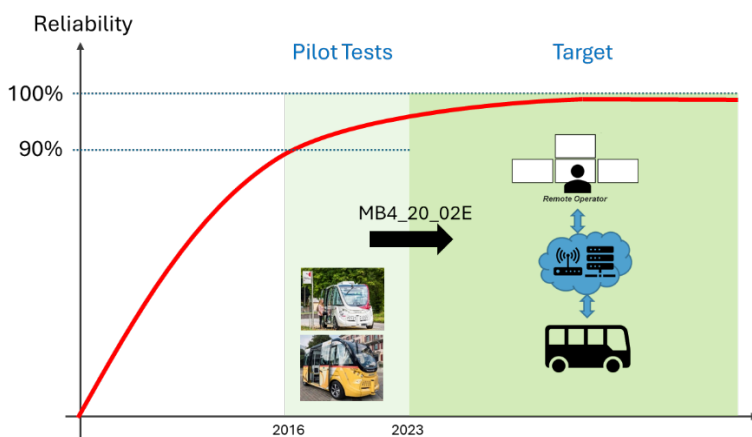


Figure 4: Transition towards automated mobility

However, Teleoperation introduces its own set of safety and security concerns, which must be thoroughly addressed to ensure the safe and secure operation of teleoperated vehicles on public roads. These concerns include the risk of cyberattacks that could compromise the control of the AV, network failures leading to a loss of communication between the AV and the Remote Operation Centre, and delays in data transmission that might affect the timeliness of Remote Operator interventions. Additionally, vulnerabilities in sensor data or Remote Operator Station interfaces could further impact the reliability and safety of the Remote Operation System (Figure 3).

This research project aims to support regulatory authorities in defining the minimum safety and security requirements necessary for the approval and operation of teleoperated AVs. These requirements will depend on various factors, including the vehicles' systems and sensors, the network infrastructure, and the Remote Operators' equipment.

The objectives of this research project are the following:

- **Objective 1:** Define minimum requirements for traffic safety, traffic flow, and IT security in a Remote Operation System.

This objective focuses on establishing the essential criteria that ensure teleoperated vehicles can be safely and securely integrated onto public roads. These criteria will address the performance and reliability of the vehicle's systems and the security of the data communication between the vehicle and the teleoperator.

- **Objective 2:** Provide the basis to better understand the limits of Remote Operation systems and to derive requirements for their evaluation and approval. This objective aims to define and better understand the boundaries and capabilities of current Remote Operation Systems, facilitating the development of comprehensive evaluation and approval processes. Understanding these limits is important to ensure that teleoperated AVs can be deployed without compromising safety or efficiency.

This document will serve as a comprehensive database enabling the selection of minimum requirements for any given ODD, scenario and level of vehicle automation. Entities wishing to deploy teleoperated vehicles on public roads should demonstrate compliance with these established requirements.

In essence, remotely operated systems are key for the broader deployment of automated vehicle fleets. Safely deploying these systems on public roads will not only improve reliability and reduce the disruptions caused by AVs but also foster public trust and acceptance of automated vehicle technology. The assurance that a human can remotely monitor AVs and provide support, if necessary, through Teleassistance or Teleoperation will significantly increase the public's trust and accelerate the adoption of AVs.

1.3 Report Structure and How to Read the Report

Figure 5 below provides an overview of the content of this research report. Its main contributions appear in chapter 2 (developing standards and norms) and chapter 4 (developing and validating the requirements).

<p>1. Introduction</p> <p>1.1 Context and Current Situation 1.2 Motivation and Objectives of the Research Project 1.3 Report Structure and How to Read the Report 1.4 What Is Not Covered</p>	<p>4. Results</p> <p>4.1 Terminology 4.2 Remote Operation Level (ROL) 4.3 Scenarios 4.4 Definition of Requirements 4.5 Requirements Validation 4.6 Testing on Site 4.7 Cybersecurity Tests</p>
<p>2. Fundamental Information</p> <p>2.1 Introduction 2.2 International and National Research 2.3 Legal Frameworks 2.4 Legal Acts 2.5 Standards 2.6 The Role of Standards in Public Procurement 2.7 Overview of Remote Operation Solution Providers 2.8 Insights from Operators in Switzerland</p>	<p>5. Identified Future Research needs</p> <p>5.1 Introduction 5.2 Identification of Research Gaps 5.3 Technical Report of the Working Group BAST 5.4 Recommendations and Prerequisites</p>
<p>3. Methodology</p> <p>3.1 Research Methodology 3.2 Research Plan</p>	<p>6. Conclusion</p>
	<p>7. Appendix</p> <p>7.1 A1 - List of Minimum Requirements 7.2 A2 - Levels of Driving Automation According to ISO/SAE PAS 22736:2021 7.3 A3 - Taxonomy of Remote Operation Levels (ROL) 7.4 A4 - Details Cybersecurity Test Results 7.5 A5 - Survey Results from LOXO Operators</p>

Figure 5: Report structure

This report is structured to provide a clear, sequential understanding of the project's objectives, methodology, findings, and recommendations, and allows for two different reading approaches:

- Readers seeking specific details are advised to refer to the table of contents for targeted sections also represented in Figure 5, while those interested in the report's high-level summary and conclusions may refer directly to the corresponding chapter **Summary** in E/D/F or to chapter **6 Conclusion**.
- Readers seeking a comprehensive view of the project's foundation are encouraged to start with the chapter **1 Introduction**, which sets the context, objectives, and overall structure of the report. Following this, chapter **2 Fundamental Information** offers an overview of relevant national and international research, providing background essential for understanding the scope and positioning of the project. Chapter **3 Methodology** outlines the approach and processes applied, while chapter **4 Results** details the used terminology, the Remote Operation Level (ROL), the scenario analyses, the identified requirements, and how to validate them. Chapter **5 Identified Future Research Needs**, contains information on the identified research questions and lists various recommendations. These chapters are intended to present the core findings in a structured and comprehensive manner.

For actionable insights, chapter **6 Conclusion** presents key recommendations and prerequisites derived from the research and analysis, aimed at guiding future work in Remote Operation Systems. Appendices and additional references at the end provide supporting documentation, detailed data, and further reading.

1.4 What Is Not Covered

While this research project addresses a wide range of topics related to the remote operation of AVs in Switzerland, certain areas are deliberately excluded from the scope to maintain focus and relevance to the objectives. Specifically, the following exceptions apply:

- **Applications on private property:** The research is concentrated on public roadways and does not extend to applications of remote vehicle operation on private property. The unique conditions and regulatory requirements of private grounds fall outside the scope of this study
- **Robots on pedestrian paths:** This project does not consider the use or operation of robots on pedestrian pathways. The focus is exclusively on vehicles operating on public roads, where traffic laws and regulations differ significantly from those governing pedestrian areas
- **Monitoring in border areas:** The monitoring of AVs is limited to Swiss territory according to the currently enacted version of “Ordonnance sur la conduite automatisée» (OCA) / “Verordnung über das automatisierte Fahren” (VAF). Problem areas arising for a variety of reasons, including international borders such as Geneva and Basel, are not considered in this study
- **On-site intervention:** As on-site intervention is part of the operational phase and is not part of the remote operation system, it does not have to be covered by the project itself
- **Homologation of AVs:** This project does not address the homologation process for automated vehicles. Ensuring that AVs possess the required hardware (HW), automation, and functionality to meet the certification standards for their respective vehicle category falls outside the scope of this study

These exclusions ensure that the research remains focus on the most critical and relevant aspects of remote vehicle operation in public spaces, aligning with the primary objectives of the project.

2 Fundamental Information

2.1 Introduction

To gain a thorough understanding of remote operated AVs and their boundaries, the subject needs to be explored from the following different angles:

- Academic and industry publications from international and national research on the technological, safety, operational aspects of remote vehicle operation, key research findings and the identified gaps in the literature
- Existing legal and regulatory frameworks that govern the use of remotely operated vehicles, with an emphasis on national and international standards
- Existing remote operation solutions offered by companies and organizations, illustrating the variety of technologies and approaches available in the market today
- Experience of vehicle operators offering practical insights and real-world perspective on the challenges and considerations involved from those who operate these systems daily

This multi-dimensional approach will yield a global overview and understanding of the subject and this foundation is essential for defining requirements in safety, security, and operations to drive AVs remotely.

2.2 International and National Research

2.2.1 Introduction

This chapter reviews a broad range of international and national research on remotely operated AVs which helps to increase the understanding of the state-of-the art and the current challenges.

2.2.2 International Projects and Papers

There are various international projects and papers that cover different aspects of remote vehicle operation. This subsection highlights a selection of state-of-the-art research papers and projects from the extensive body of available literature. The selected studies were chosen based on their relevance to key aspects of remote operation, such as communication reliability, human-machine interaction, safety standards, and regulatory frameworks. These studies not only help to understand the current technological landscape but also suggest innovative ways to address the challenges involved in Remote Operation Systems.

2.2.2.1 Remote control challenges and interface design

Felix Tener and Joel Lanir from the University of Haifa have explored the complexities of remote control for AVs. Their study, "Driving from a Distance: Challenges and Guidelines for Autonomous Vehicle Teleoperation Interfaces" [38], provides a detailed analysis based on interviews with industry experts. They identify significant issues such as latency, limited situational awareness, and the need for user interfaces that promote safe and efficient remote driving. The research emphasizes the importance of creating robust and intuitive interfaces to mitigate these challenges.

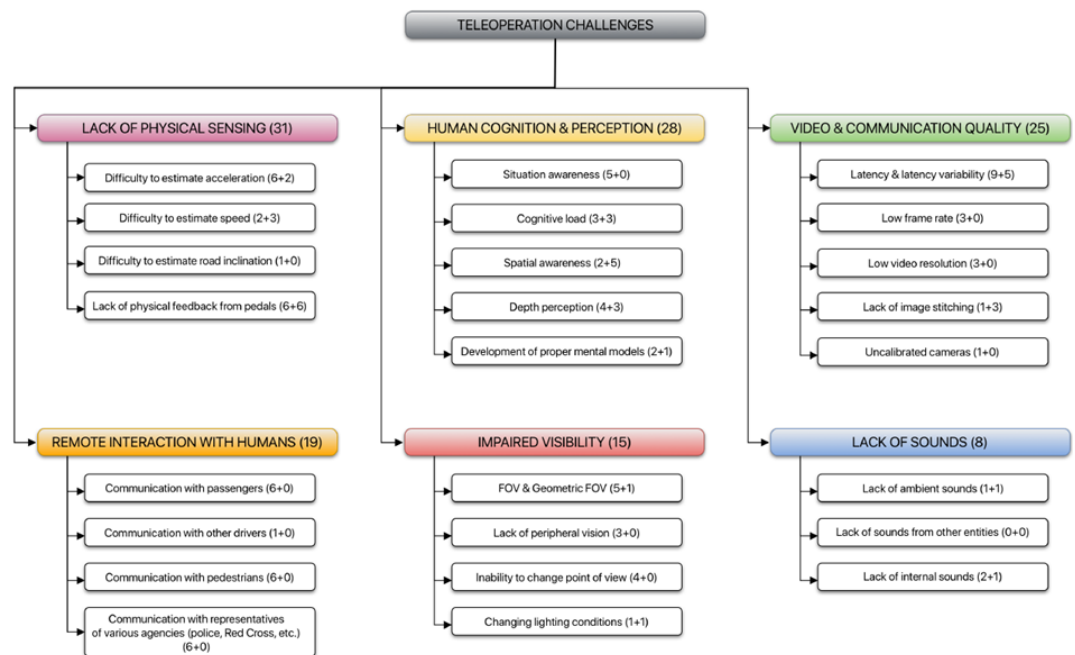


Figure 6: Categories of remote-control challenges [38]

Figure 6 above shows the categories of the main challenges described in the study. The numbers near each category name indicate how many times themes in this category appeared in the data (interviews and observations). Within the subcategories, the number of times each theme was mentioned by interviewees (left) and remote drivers (right) is displayed.

Complementing this, Gaetano Graf and Heinrich Hussmann from Ludwig Maximilian University (LMU) Munich, in collaboration with the BMW Group, conducted a study titled "User Requirements for Remote Teleoperation-based Interfaces" [39]. This research explores the needs and preferences of automotive professionals regarding remote control interfaces (Figure 7). It stresses the importance of ergonomic and safe designs that accommodate users' cognitive and physical constraints, particularly in scenarios that require quick decision-making.

User Requirements for Remote Teleoperation-based Interfaces

Gaetano Graf
BMW Group, LMU Munich
Munich, Germany
Gaetano.Graf@bmw.de

Heinrich Hussmann
LMU Munich
Munich, Germany
Heinrich.Hussmann@ifl.lmu.de

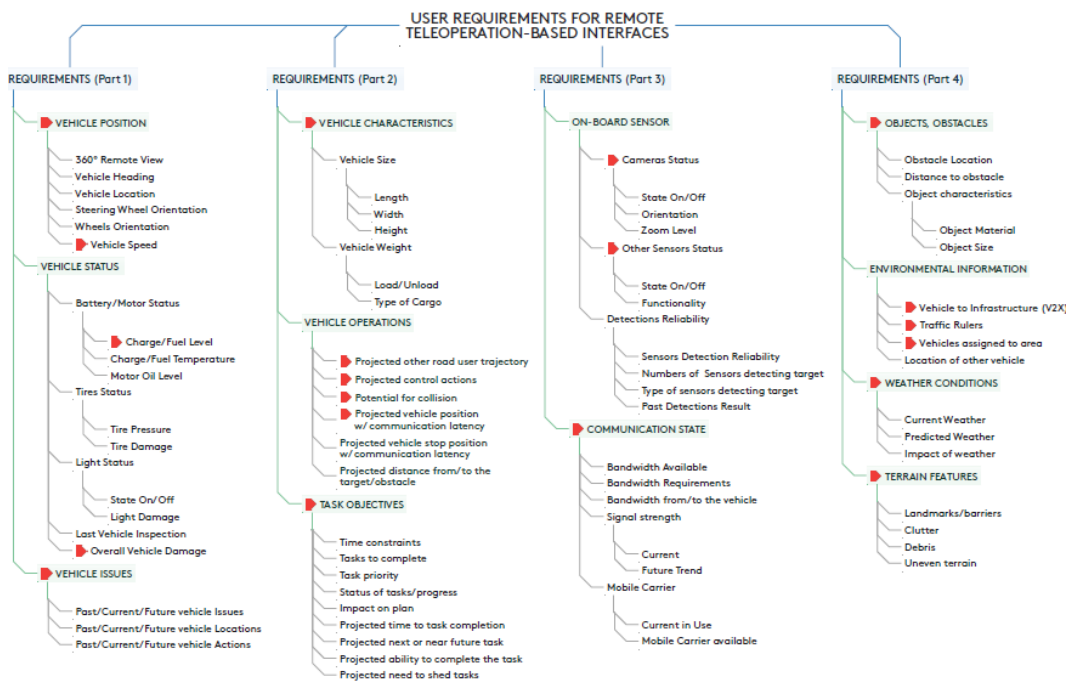


Figure 7: User requirements for remote Teleoperation-based interfaces [39]

2.2.2.2 Human performance and Teleoperation

Jessie Y. C. Chen, Ellen C. Haas, and Michael J. Barnes examine the human factors affecting remote vehicle operation in their work "Human Performance Issues and User Interface Design for Teleoperated Robots" [40]. The study reviews how elements such as field of view, orientation, and latency impact operator performance (Figure 8). The findings suggest the necessity for advanced technological solutions to overcome perceptual and control limitations, ensuring operators can function effectively even under challenging conditions.

Factor	Effects	Suggested solution
Field of View (FOV)	Erroneous speed & distance judgments; peripheral vision loss; degraded remote driving	- Increase FOV (e.g., Perspective Folding); changeable FOV can be considered - <i>Caveats</i> : perceived speed increases & motion sickness
Orientation & Attitude of the Robot	Orientation in the environment; North-up vs. Track-up map; mismatch between actual & perceived attitude of robot; unawareness of (polymorphic) robot's inclination & shape	- Map - Track-up map for navigation; North-up map for tasks involving integration of spatial relations in the environment (e.g., recon, surveying, planning tasks) - Gravity referenced view (GRV) - better awareness of robot's attitude, better route selection, and faster completion of route - Polymorphic views - operator less likely to tip the robot or have it caught on objects
Multiple Cameras	Attention switching; change blindness; perceptual registration	- Auditory alerts; multimodal solutions & visual momentum techniques
Camera Viewpoint & Frame of Reference (FOR)	Egocentric - cognitive tunneling; exocentric - loss of immediacy & true ground view; integration of info from different FORs may be challenging for operator; saliency effect	- Dual mode & inserts of other views (e.g., Sensory Ego-Sphere); peripheral cues for egocentric
Depth Perception	Underestimation of distance & size; degraded navigation, driving, & telemanipulation	- Stereoscopic Displays (SDs) - improved depth perception, obstacle avoidance, arm manipulation, important for difficult terrain & remote arm manipulation; inter-camera distance should be less than inter-ocular distance - <i>Caveats</i> : limited use - benefits mainly for difficult tasks; may induce motion sickness & perceived stress; hyper-stereo SD have multiple negative effects
Video Image/Frame Rate	Degraded motion perception & spatial orientation; degraded target identification & latency	- Minimum frame rate: 10Hz - Augmented reality/Synthetic overlay - SDs (see above)
Time Delays	Task dependent: negative effects range from 170 ms to over 1 sec; degraded driving, tracking, & telemanipulation; over-actuation when delay is variable; robot-to-operator delay more detrimental than the other direction; motion sickness; degraded telepresence	- Minimum -170 ms for driving-like tasks; other minimums task dependent - Predictive displays (e.g., Ecological Display) - navigation faster & more accurate - <i>Caveats</i> : disturbances in remote environment may make prediction model unreliable
Motion	Degradation on accuracy & latency; sometimes severe motion sickness	- Multimodal user interfaces; tailor interface to vibratory & motion effects, possible medical remediation

Figure 8: Summary of the findings regarding human performance and Teleoperation [40]

2.2.2.3 Teleoperation Taxonomy and safety

DriveU.auto is a company that has developed a comprehensive "Autonomous Vehicle Teleoperation Taxonomy" [41] with a structured framework for understanding the roles of Remote Operators and vehicles in Remote Operation Systems (Figure 9). This Taxonomy clarifies various modes of remote control, outlining the responsibilities of Remote Operators and the integration of automated systems.

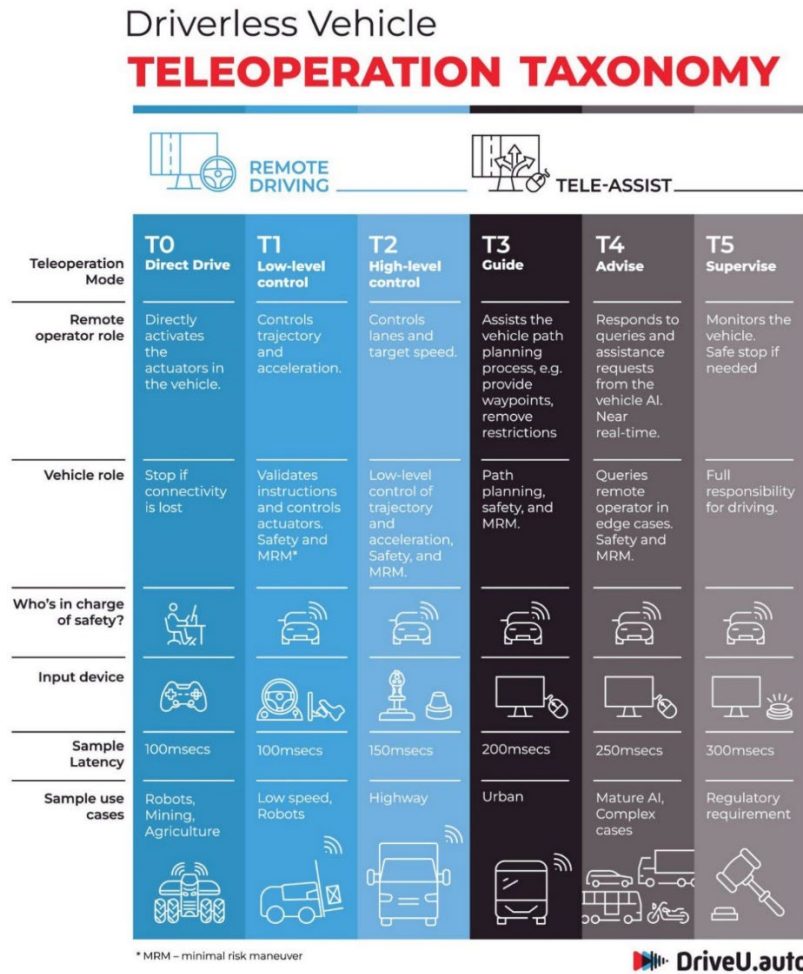


Figure 9: DriveU.auto autonomous vehicle Teleoperation Taxonomy [41]

A document made by Cruise, called the "Cruise Safety Report" [42], further explores safety protocols in the development of driverless AVs. The report details the safety methodologies employed, including design considerations, verification processes, and operational support strategies (Figure 10). Cruise's emphasis on continuous safety improvement through data-driven risk management establishes a high industry standard for other companies.

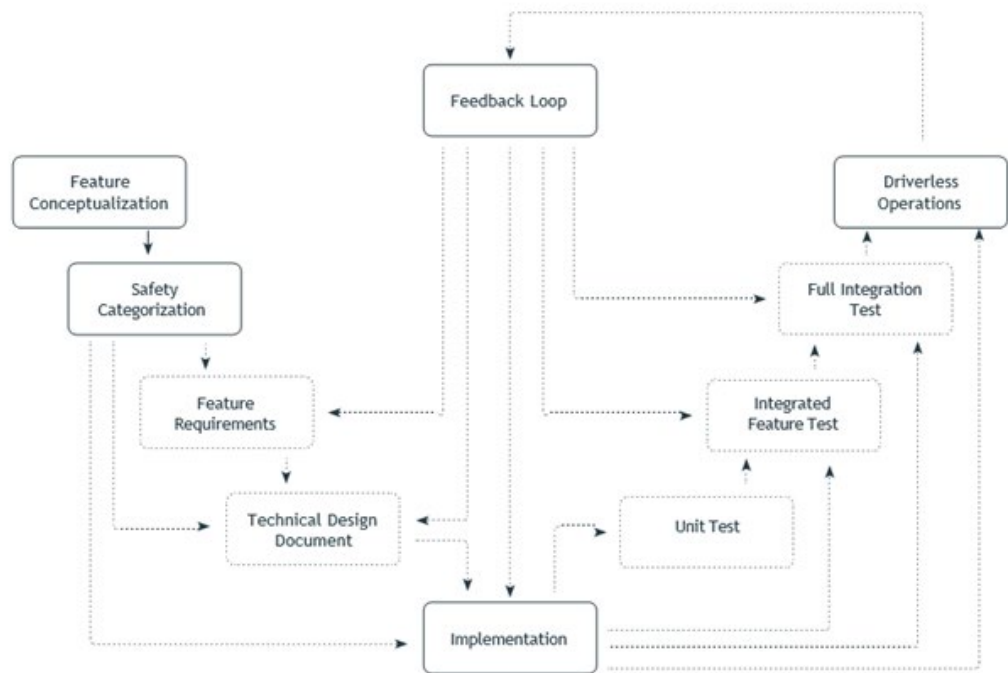


Figure 10: Cruise's system verification process [42]

2.2.2.4 Communication latency and technical supervision

Soliton Systems K.K. has addressed the issue of communication latency in remote driving within their draft “Regulations for the latency time of communication at the remote driving system” [43]. The study highlights how delays in danger recognition by Remote Drivers, compared to direct driving, result in increased stopping distances (Figure 11). This research emphasizes the importance and the need to consider latency to improve safety and operational efficiency. As illustrated in the Figure 11, the impact of latency on stopping distances decreases with lower vehicle speeds, but to achieve the same stopping distance with Teleoperation as with direct driving without latency, e.g. 12.4 m at 32 km/h, the vehicle's speed must be reduced to approximately 21 km/h when operating with 1 s latency.

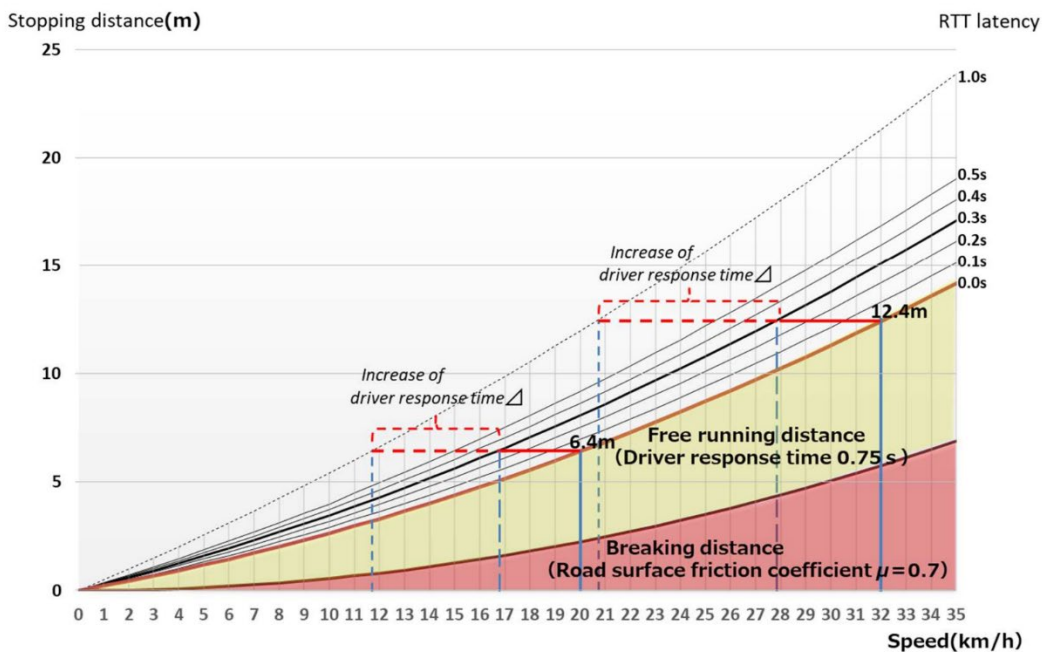


Figure 11: Stopping distance in case of remote latency [43]

The German Aerospace Centre (DLR) has contributed to research on remote operation for public transportation vehicles [44]. Their work focuses on designing a Human-Machine Interface (HMI) tailored for automated shuttles, emphasizing usability, acceptance, and workload management. The study discusses the challenges caused by technical, legal and human factors, offering insights into the iterative development of HMIs for remote vehicle supervision following the user-centred design process (Figure 12).

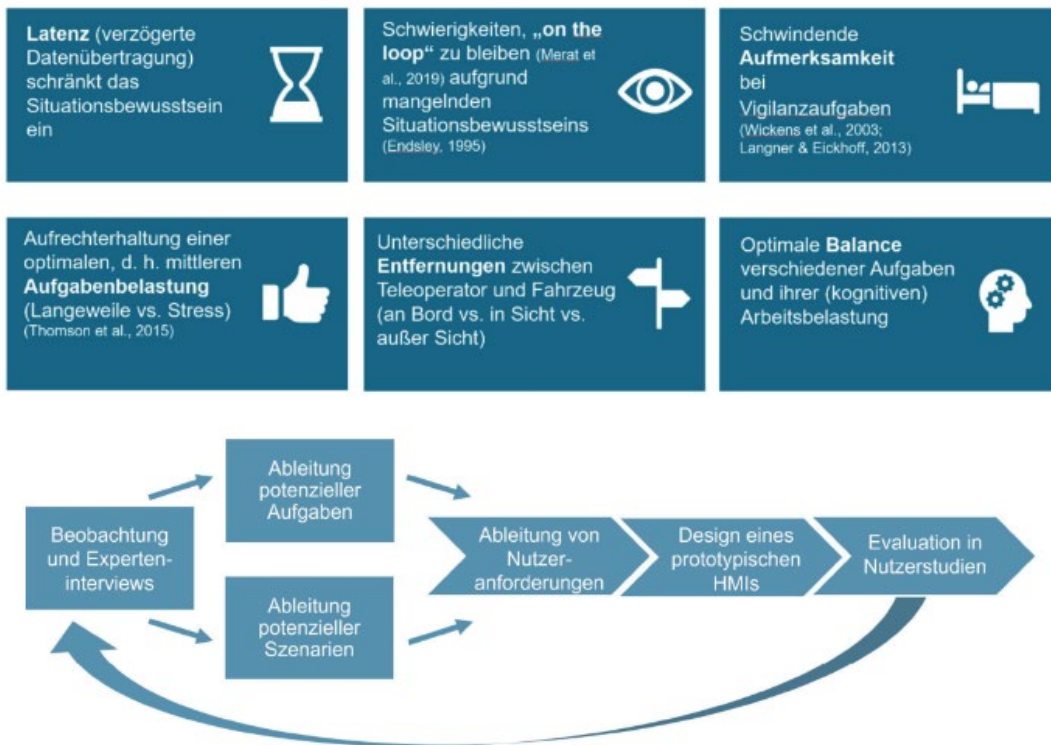


Figure 12: Process chain for designing a HMI for a Remote Operator Station from DLR [44]

2.2.3 National Projects and Papers

In Switzerland, multiple projects are advancing remote operation and the integration of automated vehicles in public transport and industrial applications.

2.2.3.1 NRP project Teleoperation – ROSAS/SwissMoves

The "Teleoperation Collaborative Project" [7], involving 12 partners of the HEIA-FR's ROSAS centre, (BFH, CarPostal, CertX, Cluster Food & Nutrition, DTC, RUAG, SBB, TPF, School of Management Fribourg and Fribourg University), focuses on developing a centralized remote-control system for Avs (Figure 13). This project aimed to create a scalable solution to improve mobility in Switzerland, particularly in public transport. It addressed technical feasibility, safety functions, and the potential for cost reduction by replacing human drivers with remote operators.



Figure 13: SwissMoves proof of concept for Teleoperation of AV [7],

2.2.3.2 Automated delivery vehicles - LOXO

The "Migronomous" project, led by Migros and LOXO [45], explores the deployment of remotely monitored delivery vehicles (Figure 14). The initiative aimed to achieve full automation in urban deliveries, enhancing safety and efficiency through ongoing remote supervision. This project represents a significant advancement towards integrating automated vehicles into everyday logistics.



Figure 14: LOXO Alpha automated delivery vehicle [45]

2.2.3.3 Industrial Teleoperation solutions

Swisscom's participation in "The Quarry of the Future" project [46] demonstrates the application of teleoperation in industrial settings. The project involves remote monitoring and control of vehicles in a dynamic quarry environment (Figure 15). The focus is on ensuring operational safety and efficiency through secure, stable, and low-latency communication solutions, which are critical in high-demand industrial applications.



Figure 15: Swisscom's monitoring solution [46]

2.2.4 Summary

Challenges overview			
Challenge Category	Specific Challenges	Description	Source/Study
Remote Operation Station interface	Latency and impact on performance	Delays in communication negatively affects the ability of Remote Driver's to respond quickly, increasing stopping distances and reducing safety.	Felix Tener & Joel Lanir, Soliton Systems K.K., Jessie Y. C. Chen et al.
	Situational Awareness and orientation challenges	Limited field of view and difficulties maintaining spatial awareness hinder Remote Operators' effectiveness in complex environments.	Felix Tener & Joel Lanir, Jessie Y. C. Chen et al.
	Ergonomic Design	Need for user interfaces that accommodate cognitive and physical constraints, especially in high-stress or quick decision-making scenarios.	Gaetano Graf & Heinrich Hussmann
	Usability and Human-Machine Interface (HMI) Design	Intuitive and robust user interfaces are essential to accommodate cognitive and physical constraints, particularly in high-stress scenarios.	Gaetano Graf & Heinrich Hussmann, German Aerospace Centre (DLR)
Human performance	Field of view and spatial orientation challenges	Restricted field of view can hinder Remote Operators' ability to effectively control AVs, especially in complex environments.	Jessie Y. C. Chen et al.
	Latency and cognitive load	Latency negatively impacts human performance, increasing cognitive load and making precise control more difficult.	Jessie Y. C. Chen et al.
Teleoperation Taxonomy and safety	Safety protocols and role clarity	Establishing clear Remote Operator roles, comprehensive safety protocols, risk management and continuous improvement strategies are crucial for safe AV use.	DriveU.auto, Cruise Safety Report
Communication and supervision	Communication latency	Minimizing delays in communication is essential for enhancing safety and operational efficiency.	Soliton Systems K.K.
	Human-Machine Interface HMI Design	Effective HMI design is critical to manage workload and ensure usability for remote supervision in public transportation and industrial settings.	German Aerospace Centre (DLR)

Table 1: Challenges overview

2.3 Legal Frameworks

2.3.1 Overview

Requirements cannot be defined without getting a basic understanding of the laws, regulations, and standards that apply to remotely driven AVs. This section looks at the legal and regulatory landscape for remote vehicle operation, breaking it down into international and national levels. It covers the main rules, laws, and standards that control how these vehicles are used and managed, pointing out the differences and details in various places.

Standards are very important in public procurement, especially in areas like transportation where safety and quality are critical. A standard is voluntary unless it is included in laws, in which case it becomes mandatory.

In the European Union (EU), harmonised European standards are developed by a European Standardisation Organisation at the request of the European Commission. These standards can be used by manufacturers or service providers to demonstrate that their products or services comply with the technical requirements of relevant EU laws. Compliance with harmonised standards grants the right to claim a presumption of conformity, effectively shifting the burden of proof. However, if a product does not conform to harmonised standards, the manufacturer must provide evidence that the product meets the legal requirements.

Harmonised standards are thus highly relevant not only for public procurement but also for the placement of products and services on the EU market. They serve as a critical tool for ensuring safety, quality, and regulatory compliance in transportation and other sectors.

They are interesting for us because they help define requirements for Remote Operation Systems on top of an existing base. By leveraging established guidelines, it is possible to ensure that the requirements are thorough, effective, and aligned with industry norms. This approach helps us create a robust framework that addresses the many aspects of remote operation, ensuring that the remote driving systems meet the highest standards of quality and reliability.

Disclaimer

As this document is not intended as a legal document, it does not offer any legally binding interpretations of the discussed regulations, standards or guidelines. The information presented in this chapter reflects the research and analysis conducted as part of the project and is intended to provide an overview of the current legal and regulatory landscape. Readers are advised to consult legal experts or authorities for guidance on the application of the discussed regulations.

2.3.2 European Union

There are various regulations, standards, or guidelines in Europe governing road vehicles, particularly automated vehicles. Figure 16 provides a brief overview of the most significant ones. It should be noted that this overview is for information purposes only and does not constitute legal confirmation or completeness. Readers should therefore not rely on the information in this overview as a legal guide and are requested to consult appropriate legal experts for binding interpretations.

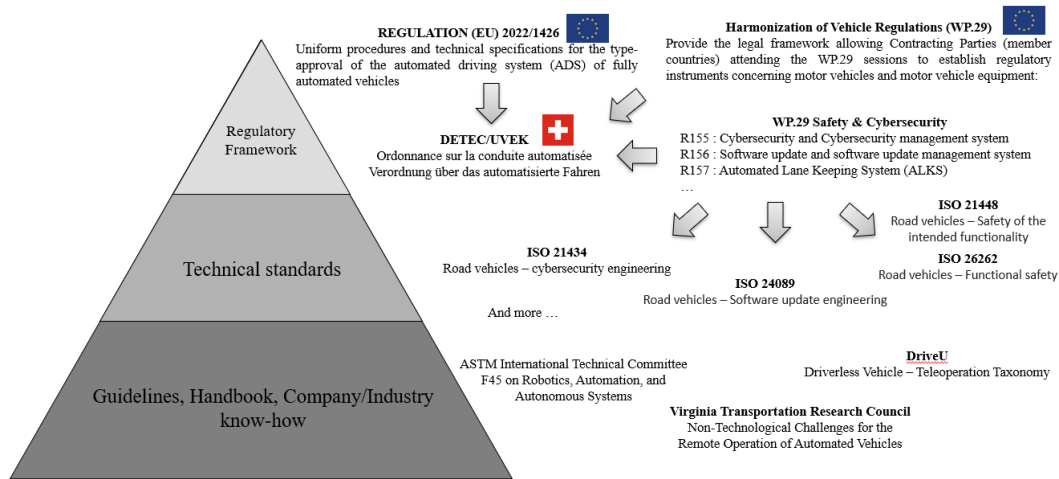


Figure 16: Overview of regulations, standards and guidelines

The European Union is working towards creating a cohesive regulatory environment for automated and remote vehicle operations. While individual member states have their specific regulations, the EU seeks to harmonize these regulations through directives and regulations that ensure interoperability and safety across borders. A significant aspect of this effort is the development of technical standards that cover various aspects of vehicle automation, including communication protocols, cybersecurity measures, and data protection.

2.3.3 International Harmonization Efforts

The development of international standards and regulations for remotely operated vehicles is also critical to facilitate international trade and ensure compatibility between different national legal systems. International organizations such as the United Nations Economic Commission for Europe (UNECE) and the International Organization for Standardization (ISO) work closely with national regulatory bodies to establish consistent, globally applicable rules for the operation of remotely operated vehicles. These harmonization efforts include:

- Safety protocols to ensure the highest safety standards for operation
- Interoperability, achieved by defining technical specifications for communication protocols, data exchange, and cybersecurity, enabling operation across various regulatory regimes
- Data protection, through guidelines for handling sensitive personal data in the context of remote vehicle operations

Such harmonization efforts are essential for enabling cross-border operations of remotely operated vehicles, ensuring they can be deployed globally without

encountering conflicting regulations. By adhering to internationally recognized standards, manufacturers and operators can ensure their vehicles comply with legal requirements across multiple jurisdictions, promoting international trade and global deployment.

2.4 Legal Acts

2.4.1 Overview

This section focuses on the legal frameworks governing remote vehicle operations, both at the international and national levels.

2.4.2 International Legal Acts

Remote and automated vehicle operations are increasingly governed by international legal frameworks designed to harmonize the regulations across different jurisdictions. These legal frameworks ensure that remotely operated AVs can be safely integrated into the global transportation system, particularly when vehicles cross borders. Standards, while generally voluntary, can support the implementation of these legal acts, as highlighted in chapter 2.3.

2.4.2.1 Geneva Convention on Road Traffic (1949)

The Geneva Convention on Road Traffic [8], adopted in 1949, serves as one of the foundational international agreements for establishing uniform traffic rules among contracting parties. While the convention predates the advent of automated and remotely operated vehicles, it laid the groundwork for subsequent legal frameworks by emphasizing the importance of driver responsibility and vehicle control.

Key points relevant to remotely operated vehicles include:

- Recognition of internationally valid driving permits, which may have implications for cross-border operation of remotely controlled vehicles
- Requirements for ensuring vehicle safety and compliance with the rules of the road, which indirectly apply to remote operators managing vehicles across borders

Although the Geneva Convention does not explicitly address automated or remotely operated vehicles, its principles influence later treaties like the Vienna Convention [9] and the development of modern international vehicle regulations.

2.4.2.2 Vienna Convention on Road Traffic (1968/2016/2021)

The Vienna Convention on Road Traffic [9], expanded on the Geneva Convention by introducing more specific provisions regarding vehicle control and driver responsibilities. Historically, the convention required that every vehicle moving on the road must have a driver at all times, which posed challenges to the development and deployment of AVs.

Recent amendments to the Vienna Convention (adopted in 2016 and 2021) have updated its provisions to accommodate new vehicle technologies, including automated

and remotely operated AVs. These updates clarify the legal status of such vehicles by allowing systems that can take over control from the driver, provided that these systems comply with national laws. The updated provisions are crucial in enabling the cross-border operation of remote and automated vehicles.

Key points of the Vienna Convention relevant to remote vehicle operations:

- The convention now permits remote control of AVs, provided that the Remote Operator is able to take over control of the AV when needed
- The responsibility of the remote operator must be clearly defined in accordance with national laws
- The convention's updates aim to harmonize the legal framework for remote vehicle operation across multiple jurisdictions, ensuring consistent rules for vehicles that operate internationally

2.4.2.3 United Nations Economic Commission for Europe (UNECE)

The UNECE is one of the five regional commissions of the United Nations and plays a pivotal role in developing international regulations for road vehicles, including remotely operated vehicles. Its subsidiary, the World Forum for Harmonization of Vehicle Regulations [47], manages the development of international vehicle regulations adopted by contracting parties.

As shown in Figure 17, six Working Parties of WP.29 are tasked with developing regulations specifically related to automated and remotely operated vehicles:

- The General Safety Provisions Group (GRSG) works on developing safety regulations that ensure vehicles meet essential safety requirements, including those applicable to remotely operated vehicles.
- The Passive Safety Group (GRSP), although primarily concerned with in-vehicle safety features like airbags and seat belts, indirectly affects remote vehicle operations by ensuring that any vehicle being remotely operated adheres to global safety standards.
- The Automated/Autonomous and Connected Vehicles (GRVA) [48] group focuses on creating safety rules for automated and connected vehicles. Its activities are guided by the framework document on Automated/Autonomous Vehicles, which sets priorities in the following in areas such as functional requirements for automated vehicles, validation methods for automated driving systems, cybersecurity and over-the-air software updates, data storage systems for automated driving vehicles (DSSAD), and remote driving systems.

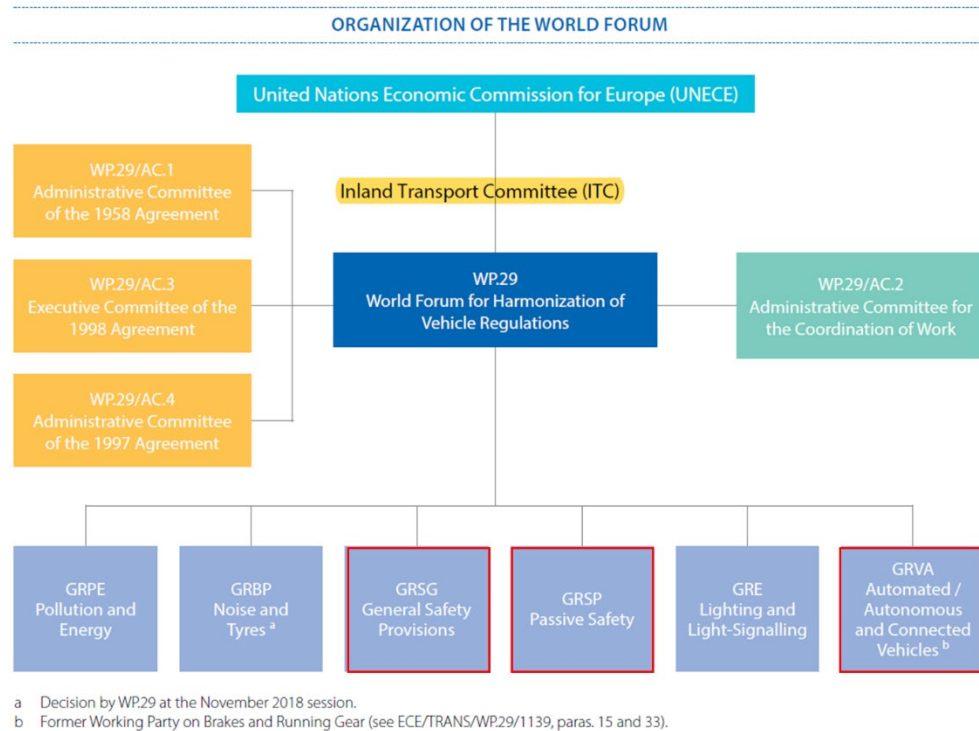


Figure 17: UNECE WP.29 organization with its 6 working parties [47]

UNECE regulations provide a comprehensive legal framework for vehicle safety and interoperability. Key UNECE regulations include:

- Regulation No. 79 [49] governs steering equipment, including the remote steering of automated vehicles. This regulation ensures that remote steering systems meet stringent safety requirements
- Regulation No. 155 (“Cyber Security and Cyber Security Management System”) [10] ensures that cybersecurity threats to vehicle systems are mitigated through robust management systems, helping to prevent unauthorized access and control of remotely operated vehicles
- Regulation No. 156 (“Software Updates and Software Update Management Systems”) [11] requires that vehicles, including those operating remotely, have a secure system for managing software updates. This is crucial for maintaining the safety and functionality of remote systems as they evolve
- Regulation No. 157 (« Automated Lane Keeping Systems (ALKS) ») [50] defines requirements for the type-approval of Automated Driving Systems (ADS) at Level 3 and above, supporting the deployment of advanced automated vehicles

While UNECE regulations provide the legal framework, ISO standards, such as ISO 23793 (Minimal Risk Manoeuvre) [51] and ISO/SAE 21434 (Cybersecurity Engineering) [52], can provide technical guidance for implementing these regulations. For example, the ISO TC 22 [53] RoSPAV Report offers a detailed overview of standardization efforts relevant to automated vehicles, which may complement UNECE’s regulatory efforts.

2.4.3 National Legal Acts

2.4.3.1 France

In France, decree no. 2021-873 [54], enacted on June 29, 2021, talks about deals with the regulatory framework for the operation of AVs. This decree, following ordinance no. 2021-443 [55], specifies the conditions under which vehicles equipped with automated driving systems can operate, including fully automated systems without a driver on board. A critical aspect of the French regulation is the requirement for a remote supervisor to monitor these vehicles, particularly when they operate on predefined routes or zones. This ensures that even in the absence of a physical driver, a human can intervene remotely if necessary.

2.4.3.2 Germany

Germany's Autonomous Driving Act [56], effective since July 28, 2021, permits the operation of SAE-Level 4 automated vehicles in designated areas without a physical driver, provided they are under technical supervision. The law mandates continuous radio communication with a remote supervisor who can intervene when necessary. It also talks about establishes the importance of the prioritization of human life in potential accident scenarios and requires comprehensive data processing regulations. Germany's regulatory framework has influenced other countries and stresses the importance of international cooperation in creating harmonized regulations for automated vehicles.

2.4.3.3 Switzerland

Switzerland's regulatory approach is now formulated in the Ordinance on Automated Driving (OCA/VAF) [3], which was adopted by the Federal Council on December 13, 2024, and will come into force on March 1, 2025 [4]. This ordinance [5] covers both partially automated vehicles requiring a driver and fully driverless vehicles. Key provisions include requirements for remote operators, who must be based in Switzerland and are responsible for overseeing the vehicle's operations, including activating and deactivating the automation systems and managing risk-reduction manoeuvres. The ordinance also mandates rigorous training for operators and requires vehicle owners to maintain the automation systems and ensure qualified personnel are available for manual operation if needed. The table below outlines relevant OCA/VAF articles pertaining to remote operation, reflecting the final ordinance text and its provisions for operational safety and governance.

Most relevant OCA/VAF articles

Reference	Designation	Summary
Art. 5	Decisive regulations	Relevant content of the technical requirements for automation systems in international regulations according to “Verordnung über die technischen Anforderungen an Strassenfahrzeuge» (VTS) / Ordonnance concernant les exigences techniques requises pour les véhicules routiers” (OETV)
Art. 33	Departure check	<ol style="list-style-type: none"> 1. Before a driverless vehicle is put into daily operation, a departure check must be carried out. 2. The departure check corresponds to a manually performed driving manoeuvre. Parts of the departure check can be carried out automatically by means of a diagnostic system. 3. The following must be checked during the departure check: <ol style="list-style-type: none"> a. The tyres and wheels as well as the suspension. b. The brakes, steering and lighting systems. c. For faults detected during the self-diagnosis: the electronically controlled vehicle systems relevant to safety and emissions.
Art. 34	Operator	<ol style="list-style-type: none"> 1. While an autonomous vehicle is in operation, it must be supervised by a human operator. 2. Operators must perform their duties in accordance with the manufacturer’s user and operation manual. Their key responsibilities include: <ol style="list-style-type: none"> a. Checking before the start of operations that the required infrastructure is available and functioning b. Activating and deactivating the automation system as specified by the manufacturer. Before activation, ensuring that the vehicle is within its approved operational area and that departure checks have been completed c. Reviewing and either confirming or overriding manoeuvres proposed by the automation system, or initiating risk-reduction manoeuvres when necessary d. Proposing driving manoeuvres to the automation system when requested e. Triggering risk-reduction manoeuvres and deactivating the automation system if required f. If a risk-reduction manoeuvre has been initiated, verifying that the cause has been resolved before resuming operation g. If the automation system initiates a risk-reduction manoeuvre, contacting passengers and implementing any measures necessary to ensure traffic safety h. Receiving and acting upon communications from passengers or third parties via the vehicle’s audiovisual interface or an alternative communication channel i. Immediately notifying the police in the event of an accident involving the vehicle on a public road. 3. Operators must carry out these tasks promptly 4. The operator’s workplace must be located in Switzerland and may be either inside the vehicle or at a remote location
Art. 35	Manual operation of a driverless vehicle	<ol style="list-style-type: none"> 1. The manual operation of a driverless vehicle may be conducted using controls located within the vehicle or through a remote-control device. 2. Anyone who operates a driverless vehicle manually: <ol style="list-style-type: none"> a. Are considered drivers under road traffic regulations. b. Are not considered Remote Operators as defined by the ordinance. 3. If the vehicle does not have conventional manual controls, manual operation is permitted only in accordance with the manufacturer’s instructions or as part of the pre-departure check process.

Reference	Designation	Summary
		4. The transition between automated and manual operation must occur only when the vehicle is stationary.
Art. 36	Requirements for the operator and the person manually driving	<ol style="list-style-type: none"> 1. The operator and the person manually driving the unmanned vehicle must: <ol style="list-style-type: none"> a. have the right to drive and the skills to drive b. while carrying out their activities, be capable of driving and free from the influence of alcohol c. have a driving license authorizing driving of vehicles of the category to which the to which the unmanned vehicle belongs, but at least category B. 2. They must have successfully completed the training and continue to educate themselves in accordance with the manufacturer's guidelines.
Art. 37	Manufacturer	<p>The manufacturer is obliged to provide training:</p> <ol style="list-style-type: none"> 1. Manufacturers must provide training for operator tasks and, if the vehicle lacks conventional controls, for manual operation. The training must cover all necessary knowledge about the vehicle's technical functionality and safe operation. 2. A certificate must be issued upon successful completion of the training. 3. If the manufacturer has no subsidiary in Switzerland, the importer may provide the training and issue the certificate.
Art. 38	Vehicle owners	<ol style="list-style-type: none"> 1. Vehicle owners shall update and maintain the automation system in accordance with the manufacturer's instructions 2. They must ensure that a departure check of the operation is carried out before daily use of the vehicle 3. They must ensure that <ol style="list-style-type: none"> a. the vehicle is only used in an area approved for that vehicle b. the AV is operated under the supervision of an operator c. the infrastructure required for the operator to carry out their tasks in accordance with the manufacturer's specifications is in place d. suitable personnel and infrastructure are available to operate the driverless vehicle manually if necessary e. the operator and the person who may operate the driverless vehicle manually have completed the necessary training f. control bodies are able to establish contact with the operator via the audiovisual interface of the vehicle 4. The vehicle owners must ensure that the obligations of the vehicle drivers are met 5. Vehicle owners are responsible for ensuring that the load is properly secured. 6. Vehicle owners must ensure that, in the event of their vehicle coming to a halt in a location that obstructs traffic, measures are taken immediately to have the vehicle removed from the carriageway by a towing or breakdown service, unless it can be moved out of the traffic area in some other way.
Art. 41	Driving mode recorder for driverless vehicles	<p>Driverless vehicles must be equipped with a driving mode recorder that logs the following events:</p> <ol style="list-style-type: none"> a. Activation or reinitialization of the automation system b. Deactivation of the automation system c. Instructions sent by the automation system to the Remote Operator d. Commands or information sent by the Remote Operator e. Risk-reduction manoeuvres executed by the vehicle f. Interruptions in the communication link between the vehicle and the Remote Operator

Reference	Designation	Summary
Art. 42	ODD	In the case of driverless vehicles, the automation system must recognise and comply with the limits of the approved area of use.
Art. 43	Application for authorisation of conditions of use	<ol style="list-style-type: none"> 3. The application must include: <ol style="list-style-type: none"> a. A description of the proposed operational areas, including routes, boundaries, challenging locations, and expected conditions b. An evaluation confirming that the operational areas align with the vehicle's design specifications, validated by the manufacturer or authorized importer c. Information on any operational limitations d. A description of the vehicle's remote intervention functions and confirmation of reliable communication with low latency across the operational areas e. A deployment concept for Remote Operators, including a declaration on how the personnel and infrastructure requirements will be met f. The EU Certificate of Conformity for the vehicle(s) and a detailed appendix on the automation system g. Consent forms from relevant parties to provide information to ASTRA as required 4. Applications for new vehicle types in already approved operational areas do not require details outlined in (3a) and (3e).
Art. 50	Execution	<ol style="list-style-type: none"> 1. FEDRO may issue instructions for the implementation of the Ordinance and in particular regulate details to ensure compliance with international and European law 2. In special individual cases, it may authorise deviations from provisions for vehicles with an automation system for driverless vehicles 3. In the cases cited in paragraph 2, it may define alternative requirements if proof is provided that a comparable level of safety is ensured 4. In the case of deviations in accordance with paragraph 2 letter d, it may limit the duration of the authorisation 5. At the request of the manufacturer or importer, FEDRO may order that, for driverless vehicles, instead of international type approvals, manufacturer's declarations of conformity with a test report are provided that it can be shown that the tests were carried out in accordance with the international regulations recognised by Switzerland 6. FEDRO shall set up a support group to assist the cantons in evaluating applications for the approval of areas of application for driverless vehicles. The support group includes representatives of the licensing authorities, the police, the authorities for construction, spatial planning and the environment, as well as other stakeholders 7. No later than five years after the entry into force of the Ordinance, FEDRO shall evaluate its effects. It shall publish the results of the evaluation

Table 2: Most relevant articles from OCA/VAF Chapter 5: Driverless vehicles [4]

The regulatory requirements in Switzerland, particularly those concerning Remote Operators, align closely with the gaps identified in international research initiatives. The research project “Auswirkungen des automatisierten Fahrens” [57] highlights that future amendments to the Swiss OCA/VAF ordinance will be necessary to better address the challenges of mixed traffic [58] and secure data management [59].

2.4.3.4 United Kingdom (UK)

The UK currently does not have a legal requirement for a driver to be physically present in the vehicle they control remotely. In February 2023, the Law Commission of England and Wales published advice recommending new legislation to address the legal complexities of remote driving [60]. The proposed changes focus on establishing accountability for remote drivers, ensuring they are responsible for their actions but not liable for issues beyond their control, such as connectivity failures. This proposal also underscores the need for international agreements to manage cross-border liability and enforcement.

2.4.4 Summary

Legal frameworks overview			
Level	Region/Country	Legal Framework/Standards	Summary
International	European Union (EU)	EU Directives and Regulations, Harmonised European Standards	The EU works towards a cohesive regulatory environment for AVs, focusing on interoperability, safety, and technical standards like communication protocols, cybersecurity, and data protection. The EU Agency for Cybersecurity (ENISA) provides guidance on general and sector-specific cybersecurity and opinion papers, including “ENISA good practices for security of Smart Cars” [61]
	Geneva Convention on Road Traffic,	adopted in 1949	Uniform traffic rules among contracting parties.
	Vienna Convention on Road Traffic	Updated 2021 to include AVs	Updates aim to clarify the legal status of AVs and set responsibilities for operators and manufacturers.
	UNECE	WP.29, GRVA, GRSG, GRSP	UNECE develops and harmonizes global vehicle regulations, in particular on AV-related regulations on road traffic rules and road traffic safety, and vehicle certification.
National	France	Decree No. 2021-873, Ordinance No. 2021-443	Regulates AV operation with requirements for remote supervision, particularly on predefined routes or zones.
	Germany	Autonomous Driving Act	Allows Level 4 AVs to operate without a physical driver under technical supervision, with emphasis on human life prioritization in accidents.
	Switzerland	Ordinance on automated driving (OCA/VAF)	Covers AVs requiring drivers and fully driverless vehicles; includes extensive regulations for operators and vehicle maintenance.
	United Kingdom	Proposed legislation (February 2023)	Recommendations focus on accountability for remote drivers and the need for international agreements for cross-border liability.

Table 3: Legal frameworks overview

2.5 Standards

2.5.1 Overview

Standards play a critical role in ensuring that remote and automated vehicle systems are developed, deployed, and operated safely and efficiently. While legal acts establish binding regulations, standards provide technical guidelines that support the implementation of these regulations. They are essential in ensuring interoperability, safety, cybersecurity, and communication among different components of the remote vehicle ecosystem. Standards can be either voluntary or mandatory when incorporated into legal frameworks, and they significantly influence public procurement and regulatory compliance.

2.5.2 International Standards (ISO)

The International Organization for Standardization (ISO) has developed key standards for automated and remote driving and are essential in supporting legal frameworks, as they provide the technical underpinnings that ensure compliance with legal requirements in different jurisdictions. By adhering to international standards, manufacturers and operators of remotely operated vehicles can ensure that their vehicles are capable of operating legally across borders, thus facilitating international trade and vehicle deployment. The following ISO standards provide essential technical foundations for automated vehicles and Remote Operation Systems:

- The ISO 26262 series (“Functional Safety”) (Figure 18) [62] focuses on the functional safety of electrical and electronic systems in vehicles, particularly in the context of automated and remote driving systems. This standard ensures that systems operate safely under all conditions and mitigates the risk of failures that could lead to accidents.
- ISO 21448 (“Safety of the Intended Functionality”, or SOTIF) [63] focuses on the safety of automated vehicle functionalities and ensures that even non-failure conditions (e.g., environmental factors or sensor limitations) are taken into account to prevent accidents.
- ISO/SAE 21434 (“Road vehicles – Cybersecurity Engineering”) [52] addresses cybersecurity engineering for road vehicles, with a focus on mitigating risks arising from cyber threats during development and throughout the vehicle lifecycle.
- ISO/IEC 27001 (“Information Security Management Systems - Requirements”) [64] addresses the security of information systems. Although primarily focused on information security management systems, it indirectly supports secure data exchange between AVs and Remote Operation Centres.
- ISO 23793 series (“Minimal Risk Manoeuvre (MRM) for Automated Driving”) [51] defines performance and system requirements for vehicles to execute a minimal risk manoeuvre in situations where automated systems are unable to continue operation safely.
- ISO/TS 23792 series (“Motorway Chauffeur Systems (MCS)”) [65] provides specifications for systems enabling automated vehicle operation on motorways, covering technical and operational requirements. Its partial relevance is more specific to motorway operations and may not apply universally to all teleoperation scenarios.
- ISO/DIS 7856 (“Remote Support for Low-Speed AV Systems - Performance Requirements, System Requirements and Performance Test Procedures”) [66]

defines requirements and test methods for remote support systems designed for low-speed automated vehicle operations. Its partial relevance lies in addressing specialized use cases for low-speed environments, which may have unique operational needs.

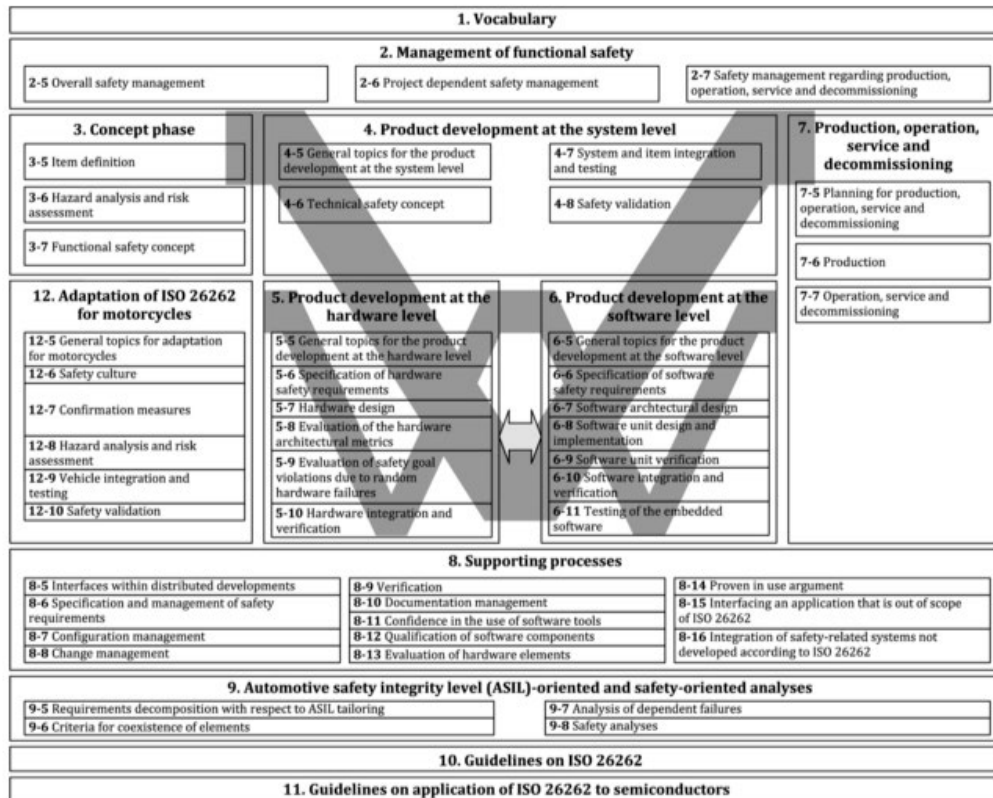


Figure 18: Overview of the ISO 26262 series of standards [62]

Additionally, the ISO/TC 22 Report on Standardisation Prospective for Automated Vehicles (RoSPAV) [67] provides a comprehensive guide to the current and future landscape of automated vehicle standardization.

2.5.3 Harmonized European Standards

In the European Union, standards are developed by European standardization organizations such as European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC), at the request of the European Commission to support the implementation of EU directives and regulations. These standards are critical for ensuring that products and services meet the technical requirements of EU law, enabling manufacturers to claim a presumption of conformity. Key standards relevant to remote vehicle operations include:

- EN ISO 21177 (“ITS Station Security Services”) enhances cooperative, connected, and automated mobility (CCAM) by securing communication between ITS stations using certificates and a public key infrastructure (PKI).
- ETSI EN 303 645 is addressing IoT devices and offers relevant cybersecurity guidelines that can indirectly support remote vehicle operations.

2.5.4 National Guidelines

In addition to international standards, many countries have developed their own national guidelines to address the specific challenges posed by remote vehicle operations. National guidelines are non-binding and serve as supplementary tools to support testing, development, and deployment of automated vehicles.

Switzerland, while closely aligned with European Union regulations and standards, has developed its own guidelines for automated and remote vehicle operations:

- **VSS (Swiss Association of Road and Transport Experts) Standards.** The VSS is responsible for developing standards related to road infrastructure and vehicle operations in Switzerland. Some relevant VSS standards address the interaction between remote-operated vehicles and road infrastructure, ensuring that vehicles comply with specific Swiss road safety guidelines.
- **FEDRO (Federal Roads Office).** As part of Switzerland’s focus on automated driving systems, the FEDRO coordinates the MB4 working group, which supports the development of guidelines and complementary standards that govern the technical specifications for remote vehicle operations. Key projects include:
 - MB4_20_02C_01 : “Cyber Threat Intelligence Framework and recommendations for C-ITS”
 - MB4_20_05E_01 : “Minimum Requirements for Infrastructure for Connected and Highly Automated Vehicles”
 - MB4_20_02E_01 : “Minimum requirements for an authorisation to remotely drive automated vehicles in Switzerland” (this project)

By aligning closely with ISO and European standards, Switzerland facilitates the safe and effective deployment of remote vehicle systems while ensuring compliance with international trade and operational requirements

2.5.5 Summary

This chapter has highlighted the role of international standards, European standards and national guidelines in supporting safe and interoperable automated vehicle operations. These frameworks collectively ensure that Remote Operation Systems meet the necessary technical, safety, and cybersecurity requirements while enabling cross-border and local deployment. Key categories include:

- 1. International Standards (ISO):** Standards like ISO 26262 (“Functional Safety”), ISO 21448 (“Safety of the Intended Functionality”, SOTIF) and ISO/SAE 21434 (“Cybersecurity Engineering”) provide foundational technical guidelines for the safe, secure and interoperable operation of AVs across different environments.
- 2. Harmonized European Standards:** Standards like EN ISO 21177 (“ITS Station Security Services”) and ETSI EN 303 645 (“Cybersecurity”) support compliance with EU regulations. They are essential for enabling cross-border vehicle operations and ensuring alignment with public procurement requirements.
- 3. National Guidelines:** While limited in scope, national guidelines complement international and European standards by addressing region-specific challenges. Examples include Switzerland’s VSS standards, which focus on road infrastructure interactions, and the guidelines developed by FEDRO’s MB4 working group. These guidelines focus on C-ITS cybersecurity, infrastructure needs for connected and automated vehicles, and safety requirements for remote-controlled Avs (this project).

2.6 The Role of Standards in Public Procurement

In the context of public procurement, standards play a critical role by ensuring that the systems being purchased meet predefined quality, safety, and technical criteria. This makes them a valuable benchmark for guiding the acquisition of products and services, including Remote Operation Systems, by providing clear and consistent requirements. Their importance lies in several key areas, as they:

- **Ensure compliance:** By referencing established standards, procurement authorities can ensure that acquired goods or services adhere to regulatory requirements and best practices
- **Simplify evaluation:** Standards provide clear, measurable criteria for evaluating bids, which streamlines the procurement process and enhances transparency
- **Promote fair competition:** Standardized requirements create a level playing field for suppliers, as all bidders are assessed against the same criteria
- **Mitigate risks:** Procurement decisions guided by standards reduce the risk of acquiring unsafe or subpar products, especially in critical areas such as automated and remote vehicle operations
- **Support interoperability:** In the case of teleoperated driving systems, adherence to international standards ensures compatibility between technologies from different suppliers, facilitating integration into existing infrastructures

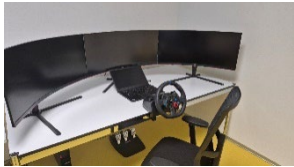


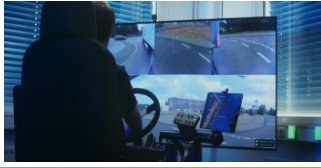


A notable example of a practical framework supporting the adoption of autonomous systems in public procurement is the BMDV's handbook on implementing autonomous vehicles in public transport [68]. This resource outlines structured approaches for planning, procurement, and deployment at the municipal level, ensuring adherence to safety, technical, and operational standards. It highlights the importance of aligning public procurement strategies with established benchmarks to simplify evaluation processes, promote interoperability, and mitigate implementation risks. By incorporating such guidelines, procurement authorities can ensure robust, scalable, and future-ready solutions for automated mobility systems.








Moreover, the adoption of internationally recognized standards ensures that systems are safe, secure, and interoperable, allowing for the expansion of remote vehicle operations on a global scale. This ensures systems are rigorously tested and certified to meet safety, security, and interoperability benchmarks before deployment.

In conclusion, while legal frameworks set the foundation for regulatory compliance, standards provide the technical backbone that supports the safe and efficient operation of Remote Operation Systems. By aligning with these standards, companies and operators contribute to building trust in the remote vehicle ecosystem through compliance with the highest safety and cybersecurity requirements.

2.7 Overview of Remote Operation Station Providers

The advancement of remote operation and automated vehicle technology is also driven by several innovative companies worldwide. These companies contribute to various aspects of technology, from software development to complete vehicle systems, offering a variety of solutions and approaches.

List of Remote Operation Station providers			
Company	Main Activity	Details	Remote Operation Setup
BFH – Berner Fachhochschule – Institute for Energie and Mobility Research	Comprehensive integration of automated driving Software and remote control solutions	Develops and integrates complete software suites for automated vehicle operations, including remote control capabilities for automated road vehicles	
Designated Driver Based in Portland, United States Founded 2018	Remote-control provider	Provides seamless remote-control solutions for both automated and non-automated vehicles, focusing on safety in challenging situations.	
DriveU.auto Based in Kfar Saba, Israel Founded 2019	Remote-control provider	Offers remote-control solutions for AVs, emphasizing safety and adaptability in diverse driving conditions.	
Fernride Based in Munich, Germany Founded 2019	Automated yard-trucking	Combines remote operation with automated technologies for sustainable logistics solutions.	
Imperium Drive Based in London, England Founded 2019	Driverless car hire service	Offers a driverless car hire service using AI (Artificial intelligence)-based predictions and link-aware streaming for remote vehicle control.	
LOXO Based in Bern, Switzerland Founded 2021	Automated delivery company	Specializes in automated delivery vehicles, leveraging low latency remote operation for smooth and safe driving	

Company	Main Activity	Details	Remote Operation Setup
Ottopia Based in Tel-Aviv, Israel Founded 2018	Remote-control software	Develops versatile remote-control software for various industries, from agriculture to logistics.	
Phantom Auto Based in San Francisco, United States Founded 2017	Remote-control software	Develops software for remote operation, particularly for logistics vehicles in complex scenarios.	
QinetiQ Based in Farnborough, England Founded 2001	Defence Technology Company	A defence technology company providing solutions across various sectors, including remote control technologies for enhanced operational efficiency and safety.	
Roboauto Based in Brno, Czech Republic Founded 2017	Software and robotics company	Focuses on technology for automated and remote-controlled vehicles, including mapping and collision avoidance solutions.	
Starsky Robotics Based in San Francisco, United States Founded 2016	Automated truck company	Focused on remote control systems for automated trucks, enabling remote monitoring and control in complex road situations.	
Teraki Based in Berlin, Germany Founded 2014	Machine learning (ML) and AI powered software	Specializes in ML and AI-powered software to manage large volumes of sensor data, applicable in remote operation contexts.	
Trilvee Based in London, England Founded 2021	Urban transport	Specializes in urban transport, blending the benefits of taxis and car-sharing with vehicle rightsizing through remote driving technology.	





Company	Main Activity	Details	Remote Operation Setup
Vay Based in Berlin, Germany Founded 2018	Door to Door Mobility Service	Plans to introduce remote operated electric cars for door-to-door mobility services, gradually incorporating automated features.	 A white, enclosed remote operation station for a vehicle. It features a steering wheel, a dashboard with multiple screens, and a person seated inside. The Vay logo and 'Teledrive Station' text are visible on the front panel.
Visteon Based in Belleville, United States Founded 2000	Development of vehicle cockpit electronics products	Develops vehicle cockpit electronics and uses remote operation to test and develop these products.	 A close-up view of a remote operation station. It shows a steering wheel and a large screen displaying a simulated road environment with other vehicles.
Voysys Based in Norrköping, Sweden Founded 2014	Remote-control software	Provides software for high-precision remote control, focusing on reliable video communication over 4G/LTE (Long-Term Evolution) networks.	 A person sitting in a remote operation station, looking at a large screen that displays a simulated road scene. The person is wearing a headset.
Zoox Based in Foster City, United States Founded 2014	AI Robotics Company	An Amazon subsidiary aiming to develop safe and efficient urban transportation solutions, utilizing remote operation to handle complex situations.	 A person operating a remote control device (a game controller) while looking at a screen that displays a simulated urban driving environment.

Table 4: List of Remote Operation Station providers

What came out from the analysis of these solutions is that the providers face several challenges. One major issue is ensuring **reliable** and **low-latency** communication between the remote operator and the vehicle, which is crucial for safety. **Cybersecurity** is another big concern, as these systems need to be protected against hacking and unauthorized access.

Integrating remote operation technologies with vehicles and existing infrastructure often requires significant customization and adaptation. Providers also have to navigate a complex landscape of national and international laws and standards that govern the use of remotely operated vehicles.

2.7.1 Summary

Challenges faced by Remote Operator Station providers

Challenge	Description
Reliable and Low-Latency Communication	Ensuring a stable and fast communication link between the remote operator and the vehicle is crucial for safety, especially in real-time remote operations.
Cybersecurity	Protecting remote operation systems from hacking and unauthorized access is a significant concern, requiring robust security measures.
Integration with Vehicles and Infrastructure	Integrating remote operation technologies with existing vehicles and infrastructure often requires extensive customization and adaptation.
Navigating Legal and Regulatory Frameworks	Providers must deal with a complex array of national and international laws and standards, which vary widely across regions and are constantly evolving.

Table 5: Challenges faced by Remote Operation Station providers

2.8 Insights from Operators in Switzerland

This section shares experiences from operators working in two different scenarios: on-board operation in a pilot project for public transport and remote operation of an AV for delivery of goods in Switzerland. The feedback from these operators gives us a clear picture of the challenges they faced and the systems they used. By understanding their day-to-day experiences, what works well and what needs to be improved has been identified. This information can help us to develop minimum requirements for remote operation systems, giving us a more complete understanding of what is really needed for safety and efficiency.

2.8.1 Feedback From an On-Board Operator of an AV for Public Transport

From 2019 to 2021, BERNMOBIL carried out a pilot test with several AVs on public roads for public passenger transport, using vehicles manufactured by EasyMile. Martin Weissen was the project manager for operations in the project. He operated the vehicle as an operator part-time, while focusing mostly on training and mentoring other operators. He ensured smooth operations by communicating across various departments and handling unforeseen events like construction site closures. He also had the role of planning and expanding the route, as well as implementing additional functions such as an on-demand shuttle service, in collaboration with EasyMile.

The route initially followed a fixed path through Bern's streets, served by shuttles during specific hours. Despite a maximum allowed speed of 30 km/h, the AV's programmed speed was much slower, facing challenges like narrow passages, confusing curves, and parked vehicles. Pedestrians, cyclists, and obstacles like vegetation further complicated operations. In the last year of its operation, the service transitioned to on-demand, covering a wider area, but faced opposition from residents due to its slow speed and disruption to narrow roads.

Various interventions were required during operations:

- Stops due to narrow road conditions or misbehaviour of other road users were frequent. The operator often had to manoeuvre the vehicle manually to create space for crossing. To solve conflicting situations, it was essential for the operator to communicate with other road users
- Manual avoidance of static obstacles, like vegetation or incorrectly parked vehicles, occurred frequently, particularly in spring and summer
- Manual bypassing of short-term construction sites was common, happening almost every round due to the project's limited area
- Emergency stops due to other road users or weather were occasional, depending on the operator's foresight and seasonal conditions
- Interruptions due to technical issues were rare but sometimes necessitated manual intervention or towing

According to the opinion of the project manager, the operator's presence for taking control of the vehicle would be necessary in every situation stated above except perhaps the emergency stops due to other road users or weather.

2.8.2 Survey Results from LOXO Operators

This section focuses on a small survey directed towards remote operators of an automated delivery vehicle. Between February 2023 and September 2023, these remote operators, associated with AMAG, vigilantly monitored and remotely piloted LOXO's vehicles, reshaping the paradigm of goods delivery in the Ebikon region. The complete results of the survey are available in the chapter 0.

The feedback collected from operators about the remote operation system provided an interesting view of both its strengths and areas for improvement. Below are the different aspects examined in the survey (Note that the values of the ratings have a maximum value of 5).

- 1. Remote Operation Design and Interface:** Operators generally thought the remote operation system was well designed. The clarity and intuitiveness of the screen and tablet positioning were noted positively. The screen sizes were seen as adequate, and the overall ease of use was highly regarded. However, the tablet interface, especially for tasks like order allocation, received some lower ratings. The button layout on the steering wheel also showed room for improvement.
- 2. Transition Between Modes and Visual Feedback:** Switching between Teleoperation and automated modes was considered moderately intuitive. The camera views and augmented reality (AR) features, like guiding lines, suggested that these visual aids could be better.
- 3. Technical and Physical Setup:** Feedback on the technical setup and ergonomics of the Teleoperation Control Centre (TCC) was mixed. Many operators found the arrangement of seats, steering wheel, pedals, and screens comfortable, but there were issues, especially with the seating height and video screen quality. Comments mentioned that the pedals felt somewhat cheap and lacked good feedback, and the steering wheel could use clearer labelling of buttons.
- 4. Sound and Distraction Management:** Soundproofing in the TCC indicated a need for better isolation from external noises. The TCC's isolation from disruptions, like people entering the room, was also noted as needing improvement. Common distractions included interruptions from people asking questions or making phone calls during operations, highlighting the need for better distraction management.
- 5. Recommendations and Cybersecurity:** Operators suggested several improvements, including improving camera resolution and reducing lag, offering personalized configurations for each teleoperator, and improving AR features using LiDAR data. The need for sound feedback and a more intuitive interface was also mentioned. Regarding cybersecurity, awareness of incident response plans was low. Moreover, 64% of respondents indicated they had not received cybersecurity training, pointing to a significant gap in preparedness. However, the availability of a help desk was highly appreciated, suggesting that additional support structures are valuable for operators.

The feedback reveals that while the remote operation system is functional and user-friendly, significant improvements are needed in areas such as visual quality, ergonomic design, soundproofing, and cybersecurity training. Addressing these issues will enhance the overall efficiency and safety of remote vehicle operations. These areas are also great indicators as to where to focus on regarding the creation of the

requirements, ensuring they meet the minimum standards for great driving experiences.

2.8.3 Summary

Overview of the experiences of operators in Switzerland		
Experience Subject	Description	Challenges/Insights
On-Board Operation (Public Transport AV)	Pilot test using EasyMile AVs on public roads in Bern for public passenger transport (2019-2021).	Frequent manual interventions were needed for narrow roads, static obstacles, and construction sites; operator presence was crucial.
Manual Interventions Required	Operators had to manually manoeuvre vehicles in tight spaces, avoid static obstacles, and bypass construction sites.	Required due to narrow roads, misbehaving road users, vegetation, and parked vehicles.
Direct communication with other road users required	Operators had to use hand signals to avoid deadlock situations.	Required because other road users cannot anticipate the behaviour of the AV.
Transition to On-Demand Service	The service expanded to cover a larger area with an on-demand model.	Faced opposition from residents due to slow speed and road disruption.
Emergency Stops and Technical Issues	Emergency stops were occasionally necessary due to road users or weather, and rare technical issues required manual intervention or towing.	Operator intervention was generally necessary, except for some emergency stops.
Remote Operation (Goods Delivery AV)	Survey of AMAG operators monitoring LOXO's remote-operated delivery vehicles in Ebikon (Feb-Sep 2023).	Revealed mixed feedback on system design, ergonomics, and transition between modes.
Remote Operation Design and Interface	Operators found the system generally well-designed with adequate screen size, but some issues with tablet interface and button layout.	Improvement needed in tablet interface and steering wheel button layout.
Transition Between Modes and Visual Feedback	Moderately intuitive switch between teleoperated and automated modes, with AR and camera views needing enhancement.	Better visual aids and smoother transitions between modes required.
Technical and Physical Setup	Mixed feedback on ergonomics; issues with seating height, video screen quality, and pedal feedback were noted.	Ergonomic improvements, better pedal feedback, and clearer button labeling needed.
Sound and Distraction Management	Issues with soundproofing and managing distractions in the TCC were highlighted.	Better sound isolation and distraction management required.
Recommendations and Cybersecurity	Operators suggested improvements in camera resolution, AR features, and cybersecurity awareness.	Cybersecurity training and personalized configurations are necessary; help desk availability was appreciated.

Table 6: Overview of the experiences of operators in Switzerland

3 Methodology

3.1 Research Methodology

This section describes the specific research methodology employed to investigate the remote operation of AVs. The methodology was designed to systematically address the research questions, ensuring that the findings are both reliable and valid. This includes a detailed explanation of the data collection methods, the analytical approaches used, and the criteria for validating the results. By adhering to a rigorous methodological framework, the project ensures that the conclusions drawn are well-founded and applicable to real-world scenarios.

The definition of the minimum requirement criteria for teleoperated driving was based on findings from pilot tests with the vehicles from LOXO and the BFH (Bern University of Applied Sciences). This showed that a clear definition of terminology is necessary to ensure that the criteria can be checked for completeness in selected scenarios.

The research methodology followed a structured research plan organized into distinct Work Packages (WPs), which are detailed in chapter 3.2. These WPs provided a systematic framework for addressing the project's objectives comprehensively. Validation of requirements was a critical element, incorporating three key methods: comparison with existing standards, scenario-based validation, and performance validation through theoretical, experimental, or literature-based approaches (see chapter 4.5).

Expert interviews formed a key component of the methodology, contributing valuable practical insights throughout the process. These interviews, conducted with stakeholders from academia, industry, and regulatory bodies, informed the scenario definition, requirements validation, and final recommendations.

To ensure a thorough investigation, the process was divided in six key phases:

- 1. Initial Definition Phase:** This phase established the core definitions and terminology necessary for the project. Definitions were agreed upon during internal workshops and validated through a literature review.
- 2. Literature Review and Requirements Collection:** A thorough literature review was conducted to collect studies, standards, and publications relevant to teleoperated driving. This phase identified a broad set of potential requirements, which were consolidated and categorized during workshops with the project team.
- 3. Scenario Definition and Interviews:** Scenarios were defined using expert interviews and internal workshops. Vehicle dynamics, safety parameters, and operational contexts were analysed to identify representative scenarios. Eight scenarios were selected for further analysis.

4. Testing and Validation:

Multiple types of tests were conducted to validate the defined requirements:

- **Operational Tests:** Practical tests, described in Chapter 4.6, were carried out using vehicles from LOXO and BFH. These tests evaluated Teleoperation capabilities, including communication reliability, system latency, and vehicle manoeuvrability under various conditions. Results from these tests directly informed the refinement of requirements
 - **Cybersecurity Testing:** As detailed in chapter 4.7, these tests formed a crucial part of the validation methodology. They assessed the robustness of the proposed cybersecurity requirements, focussing on standards like ISO 21434 and UNECE Regulation No. 155. The tests also addressed specific challenges in securing data exchanges and protecting Remote Operation Systems against unauthorized access
5. **Requirements Refinement:** Based on feedback from tests, interviews, and scenario analysis, the initial list of requirements was refined into a condensed, prioritized set of minimum requirements.
6. **Expert Consultations:** Throughout the project, expert interviews ensured alignment with practical realities.

When validating the requirement criteria, particular attention was paid to whether they were defined directly or based on existing standards and regulations. Contrary to original expectations, most of the requirement's criteria could be validated on this basis. The remaining criteria, which could not be based directly on standards, were developed based on experience with the two vehicles from LOXO and BFH. As these vehicles were already operational, their performance provided a reliable basis for validation

For criteria without direct empirical values, calculations and expert estimates were used. The effects of the presumably most significant of these assumptions were checked and validated during tests on the DTC test site in Vauffelin with the two vehicles and Remote Operation Centres from LOXO and BFH.

The list of minimum requirement criteria was continuously reviewed and adjusted as necessary. Care was taken to ensure that no contradictory or redundantly formulated criteria were included.

3.2 Research Plan

The development of minimum requirements for teleoperated driving systems involves a complex interplay of technological, regulatory, and operational challenges. To address these effectively, this project was structured into three interconnected phases, each building on the previous one to ensure a comprehensive approach to identifying, validating, and refining the requirements for Remote Operation Systems. This structured approach not only ensures alignment with international standards and industry best practices but also integrates insights from real-world testing and expert consultations. The aim was to create a robust framework for defining minimum requirements that are practical, implementable, and applicable across diverse use cases.

This project was divided in the following three main parts:

- Definition of requirements (WP2)
- Validation of requirements (wp3)
- Analysis and Recommendation (WP4)

The research plan in Figure 19 below summarizes these three parts together with the Work Package 1 (WP1: “**Organization and Coordination**”).

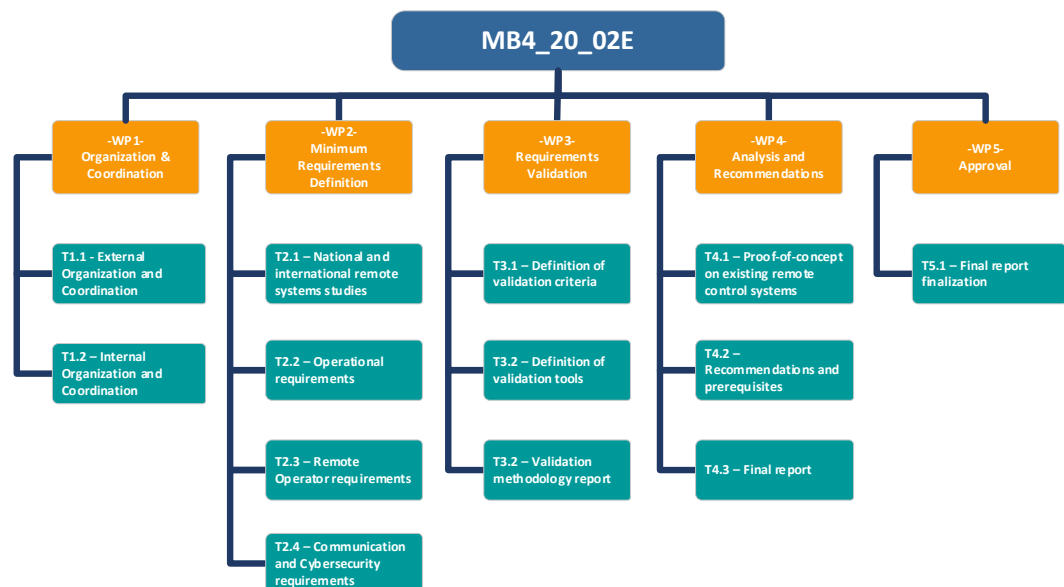


Figure 19: Project overview with work packages

The first phase (WP2: “**Minimum Requirements Definition**”) consisted of collecting studies, publications, papers, standards and guidelines published in Switzerland and Europe. This approach established a common knowledge base for proceeding further. This in turn enabled the collection and elaboration of requirements for Remote Operation Systems which include all the technical requirements for the Remote Operation Centre, the ODD, the exchange of private data and the Remote

Operator as well technical requirements for AV functional safety and cybersecurity technologies.

The second phase (**WP3: “Requirements Validation”**) consisted of defining a methodology for verifying and validating the requirements for Remote Operation System according to the requirements defined in the first phase. The first step involved defining the criteria to validate the fulfilment of requirements. This process combined insights from several sources: a review of existing literature, results from prior and project-specific tests, as well as the expertise of the project team. Additionally, workshops were conducted to discuss and refine these criteria. During these workshops, preliminary values were proposed and assessed for their practicality and alignment with real-world constraints. Whenever possible, numerical thresholds were derived from established standards and previous empirical data. For requirements lacking direct references in the literature or standards, estimates were made based on expert judgment and validated through iterative testing. A requirements validation tool was then created along with documentation explaining the procedure to follow for an entity wishing to deploy a remote vehicle control system.

The third and last phase of the research project (**WP4: “Analysis and Recommendations”**) tested the proposed requirements validation tool and the associated procedure on the Remote Operation System of an existing AV. BFH and LOXO provided their Remote Operation Centres and AVs (Figure 20), and the Dynamic Test Centre provided the test track (Figure 21). The results of these tests are not intended to validate an existing Remote Operation System, but to determine whether the requirements validation tool and procedure proposed in the previous phase are applicable to real Remote Operation Systems.



Figure 20: LOXO's Remote Operation Centre



Figure 21: Dynamic Test Centre's test track

4 Results

4.1 Terminology

4.1.1 Introduction

In automated and teleoperated driving, terminology can vary across scientific literature and technical standards. This section provides clear definitions of terms for a Remote Operation System such as the one shown in Figure 22 to ensure consistency and clarity in the current project and with the list of definitions.

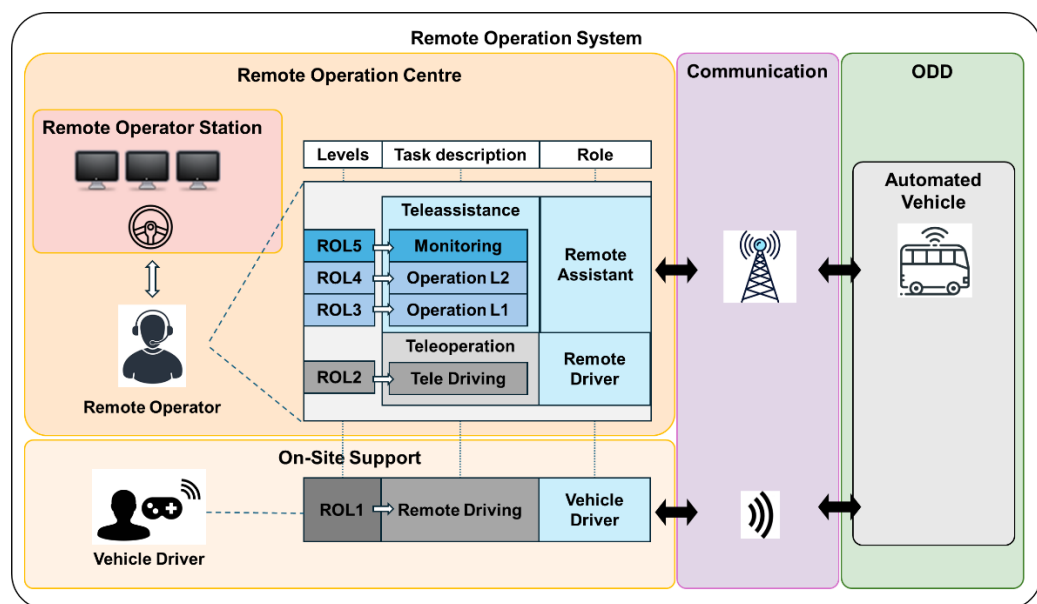


Figure 22: Remote Operation System with tasks and roles

4.1.2 Definitions

The definitions are presented in alphabetical order, and where applicable, the sources or standards are cited. The document “Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles” [69] provides a comprehensive overview on this topic.

- **Automated Driving System (ADS):** A set of elements that offer a specific conditional or higher automated driving use case in or for a specific ODD (ISO 4808).
- **Automated Vehicle (AV):** A vehicle capable of sensing its environment and moving safely with no direct human input, designed to be operated by automated driving systems at levels 4 and 5 as defined by ISO/SAE PAS 22736:2021 (see Appendix 7.2). The AV is referred to in the OCA/VAF ordinance as 'Operator' in German and 'conducteur' in French. The AV is referred to as “führerloses Fahrzeug: Fahrzeug mit einem Automatisierungssystem” in German and “véhicule sans conducteur: un véhicule équipé d’un système d’automatisation” in French in the OCA/VAF ordinance.

- **Direct Control:** Remote Operator acting as Remote Driver in Remote Operation Level (ROL) ROL2 and Vehicle Driver acting as Remote Controller Driver in ROL1.
- **Dynamic Driving Task (DDT):** All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including, without limitation, as defined by ISO/SAE PAS 22736 (see Appendix 7.2).
- **Dynamic Driving Task (DDT) Fallback:** refers to the response by the user to either perform the DDT or achieve a minimal risk condition in two situations: (1) after the occurrence of a DDT performance-relevant system failure(s), or (2) upon exiting the ODD. Alternatively, it refers to the ADS's response to achieve a minimal risk condition under the same circumstances (Figure 23).

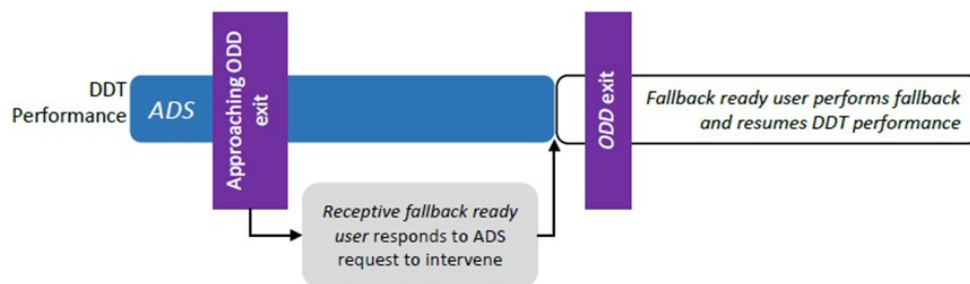


Figure 23: Sample Use Case sequence DDT [69]

- Sample use case sequence at Level 3 showing ADS engaged and occurrence of exiting the ODD that does not prevent continued DDT performance. User performs the fallback and resumes DDT performance.
- **Driver:** A user who performs parts or all of the DDT and/or DDT fallback in real-time for a particular vehicle (ISO 4808).
- **Driver Support System:** A driving automation system that can only perform part of the DDT (ISO 4808).
- **Failure Mitigation Strategy:** A vehicle function designed to automatically bring an ADS-equipped vehicle to a controlled stop in response to (1) a prolonged failure of the fallback-ready user of a Level 3 ADS feature to perform the fallback after the ADS has issued a request to intervene, or (2) a system failure or external event so catastrophic that it incapacitates the ADS, making it unable to perform vehicle motion control to achieve a minimal risk condition Defined in [69].
- **Latency:** The time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port (Request for Comments (RFC) 1242).
- Relevant Latency Measures for Tele-operated Driving (ToD) – see also Figure 63:
 - **Uplink Video Latency (Glass to Glass):** Latency from on-board video capture to Remote Operator Station, including video encoding and rendering
 - **Uplink Data Latency:** Travel time of data from vehicle to Remote Operator Station
 - **Downlink Data Latency:** Travel time of data from Remote Operator Station to vehicle
 - **Roundtrip Latency:** Sum of uplink video and downlink data latency

- **Service Level Latency:** Total latency from event occurrence to activation of actuators, including video encoding and rendering and reaction time of Remote Operator
- **Reliability:** The ability of an item to perform a required function under given conditions for a specified period of time (ISO 26262).
- **Remote Vehicle:** A Remote Vehicle refers to an Automated Vehicle (AV) that can be supervised or controlled remotely through Teleassistance (ROL3-ROL5), Teleoperation (ROL2) or Remote Controller Driving (ROL1). In the context of this project, it represents a key category within the requirements framework, addressing the specific needs and functionalities of AVs as part of a Remote Operation System.
- **Minimal Risk Condition (MRC):** A stable, stopped condition to which a human driver (Remote Operator acting as Remote Driver) or automated driving system brings a vehicle after performing a Minimal Risk Manoeuvre (MRM) to reduce the risk of a collision or other loss when a given trip cannot be continued (The British Standards Institution BSI, 2023).
- **Minimal Risk Manoeuvre (MRM):** A tactical or operational manoeuvre triggered and executed by the driving automation system or the human driver (Remote Operator acting as Remote Driver) to achieve the MRC. This can also include the action of a Remote Driver (The British Standards Institution BSI, 2023). A more detailed definition is given in 6.0.
- **Operational Design Domain (ODD):** The operating conditions under which a given driving automation system or feature is specifically designed to function, including environmental, geographical, and time-of-day restrictions, and the requisite presence or absence of certain traffic or roadway characteristics [69].
- **Object and Event Detection and Response (OEDR):** Subtasks of the DDT that include monitoring the driving environment, detecting, recognizing, and classifying objects and events, preparing to respond as needed, and executing an appropriate response to such objects and events to complete the DDT and/or DDT fallback [69].
- **Remote Driver:** This is a specific role of the Remote Operator, who is responsible for the active remote control of an AV in real time. This role applies primarily to Teleoperation in ROL2, where the Remote Driver takes direct remote control of vehicle functions, including steering, acceleration, and braking.
- **Remote Driving:** This involves the remote driving of an AV in ROL1, where a Vehicle Driver controls the AV via an on-site remote controller.
- **Remote Operator:** A Remote Operator is an individual who oversees or interacts with a Remote Operation System to ensure the safe and efficient functioning of an AV. Depending on the Remote Operation Level (ROL), the Remote Operator may take on different roles, such as a Remote Driver (ROL2) or Remote Assistant (ROL3-ROL5). The Remote Operator is referred to as 'Operator' in German and 'conducteur' in French in the OCA/VAF ordinance.
- **Remote Operator Level (ROL):** Defines the varying roles of the Remote Operator while performing tasks to supervise (ROL5), assist (ROL3-ROL4) and take temporary over the control of an AV (ROL2). In ROL2, the Remote Operator acts as a Remote Driver, performing tasks of Tele Driving.
- **Remote Operation Centre:** A centre that includes the necessary infrastructure such as Remote Operator Station and communication to monitor AVs, support

them (ROL3-5) by Teleassistance and also control them temporarily via Teleoperation using direct control (ROL2).

- **Remote Operation System:** A system consisting of a Remote Operation Centre, the Automated Vehicle and the Communication Infrastructure between them.
- **Scenario:** A sequence of scenes integrated with the ADS(s)/subject vehicle(s) and their interactions in the process of performing certain Dynamic Driving Tasks (ISO 34503).
- **“False positive” Scenario:** a "False Positive" occurs when the perception system of an automated vehicle correctly detects an existing object (such as a tree branch, trash, or small debris) but inaccurately classifies it as a critical obstacle that requires the vehicle to stop or take evasive action.
- **Taxonomy:** A Taxonomy is a structured classification system that organizes concepts or processes into defined categories or levels. In this report, the Taxonomy is used to clearly define and distinguish various Remote Operation Levels (ROL) and their functionalities, providing a consistent framework for analysis and discussion.
- **Teleassistance Operation L1:** A Remote Operator acting as Remote Assistant in ROL3.
- **Teleassistance Operation L2:** A Remote Operator acting as Remote Assistant in ROL4.
- **Teleoperated Driving (ToD):** Teleoperated Driving refers to the act of driving a vehicle where part or all of the tasks are performed by a remote operator, usually over wireless communications (5GAA Automotive Association, 2021). Corresponds to ROL2.
- **Tele Driving:** Teleoperation of an AV in ROL2 where a Remote Operator acts as Remote Driver.
- **Teleoperator:** A Remote Operator without direct vision but with tele-transmitted information (e.g., by cameras) (ISO 4804).
- **Teleassistance:** Remote Operator acting as Remote Assistant in ROL3-ROL5. Teleassistance is an emerging concept in automated driving and focuses on providing different levels of guidance or support without taking full vehicle control to automated systems. With this fallback it is possible to ensure the vehicle can be operated safely even when it encounters situations beyond its automated capabilities.
- **Teleoperation:** Teleoperation, or Tele-operated Driving (ToD), allows a Remote Operator to directly control an automated vehicle (AV) when necessary, specifically in ROL2 situations. This process, also known as Tele Driving, serves as a safety mechanism to handle complex or unexpected driving scenarios that the automated vehicle cannot manage on its own and that cannot be resolved through Teleassistance.
- **Teleoperation Control Centre (TCC):** A Remote Operation Centre which is also equipped to perform Teleoperation (ROL2)
- **Operator:** A designated person, appropriately trained and authorized, to operate the vehicle (ISO 4804).
- **Use Case (UC):** A specification of a generalized field of application, possibly including information on the system for one or several scenarios, the functional range, the desired behaviour, and the system limits (ISO 4804).
- **Vehicle Driver:** This is a specific role of a person, who is responsible for the active direct control of an AV in real time using an on-site remote controller. This role applies primarily to ROL1, where Tele Driving is not possible and the Vehicle

Driver needs to take direct control of vehicle functions, including steering, acceleration, and braking.

4.1.3 Minimum Risk Manoeuvre (MRM)

According to ISO/SAE PAS 22736, the Minimum Risk Manoeuvre (MRM) is a critical functionality within an ADS that aims to achieve a Minimal Risk Condition (MRC), the foundational safety mechanism of an AV system, ensuring the protection of both the vehicle and other road users by bringing the vehicle to a stable, minimal risk condition (MRC) in challenging or failure scenarios. It differs from a "Failure Mitigation Strategy," which involves bringing the vehicle to a stop under specific conditions, and from collision mitigation systems that focus on minimizing collision risks during normal operations. The standard also outlines the classification framework for MRM types, decision-making processes, and minimum requirements for control strategies and testing procedures.

The MRM function acts as a fallback mechanism when the ADS encounters events that prevent it from continuing the dynamic driving task. These events may include failures in the automated driving system or its components, risks of exiting the ODD, or the failure of a remote operator to respond to a transition demand. MRM is integrated within the ADS, selecting the most appropriate type based on the vehicle's state and other factors.

From a functional safety perspective, MRM is essential starting from Level 3 conditional automated driving, where the ADS can perform the complete dynamic driving task. It ensures safe operation during critical conditions when the driver or remote driver may not be able to retake control.

The European Association of Automotive Suppliers (CLEPA) and the International Organization of Motor Vehicle Manufacturers (OICA) endorse MRM as an automated procedure to mitigate risks in traffic in situations like the aforementioned.

Types of MRM:

- **Emergency stop (abrupt deceleration):** Initiated in response to critical failures or imminent risks. Involves rapid deceleration to bring the vehicle to a standstill.
- **Gradual deceleration, lane change and controlled, safe stop:** Triggered when the ADS detects potential risks that can be managed through controlled deceleration, lane change and a carefully executed safe stop (e.g. on the emergency lane or the side of the road). This type of MRM is crucial for ensuring the safety of both the vehicle and other road users by avoiding abrupt stops while enabling smoother and safer transitions in traffic.
- **Traffic-aware manoeuvre:** Considers surrounding traffic conditions. Involves adaptive manoeuvres to navigate through traffic and reach a minimal risk condition.
- **Fallback to predefined safe area:** Initiated when the ADS is at risk of exiting its ODD. Involves guiding the vehicle to a predefined safe area.

4.1.4 Use Cases and Applications

Remote vehicle operation has a wide range of applications across different fields which can be broken down into areas like mobility, agriculture, airports, mining, and logistics [70]. Each of these has its own set of challenges and opportunities. This wide range of use cases shows just how flexible and useful remote vehicle control can be, especially in complicated situations where regular driving might not be safe or possible.

It should be noted that the requirements listed in this report become relevant in the following use cases whenever an AV is driven on public roads.

Mobility Use Cases	
Use Case	Description
Remote driving in edge cases	Remote guidance of vehicles from a control centre during challenging situations, such as inner-city traffic, changing road layouts, or adverse weather conditions.
Remote valet parking	A remote operator parks the vehicle using real-time video streaming from the vehicle, providing convenience and efficiency in parking services.
Driving responsibility turnover	On-demand transfer of driving responsibilities to a remote operator, enabling a modified taxi economy through digitalization.
Transport for disabled/senior people	Enhances mobility for senior citizens and handicapped individuals by enabling remote-controlled vehicle operation.
Robotaxis	Teleoperated driverless taxis operated by ride-sharing or taxi companies from remote tele-operation Centres, offering an automated transport solution.
Transport shuttles	Remote control of driverless shuttles for public transport, enhancing safety and efficiency in passenger movement.
Automatic valet parking	Remote driving Centres provide pathways for vehicles to automatically park in designated spots, optimizing parking space utilization.
Platooning	A pilot/escort vehicle, driven remotely, leads a group of vehicles, functioning as a Remote Control Centre and ensuring coordinated movement.
Fleet management	Centralized remote control of vehicle fleets, ranging from electric vehicles on university campuses to large-scale public transport systems, enabling efficient fleet operations.
Remote vehicle delivery/renting	Vehicles are delivered directly to customers for rental or sharing purposes, facilitated by remote control, enhancing convenience and operational flexibility.

Table 7: Mobility Use Cases

Agriculture Use Cases

Use Case	Description
Situational assistance to automated tractors	Remote guidance of automated tractors from remote centre during difficult situations such as changing fields, bad weather, etc.
Remote controlled tractors/harvesters	Direct remote control of tractors or harvesters from a remote operation centre.
Weeding robots	Remote control of robots used for removing weeds or unwanted plants in the fields.
Remote controlled grass cutters	Remote control of machines for cutting grass in agricultural fields and in forestry applications.
Remote control tool carrier	Remote control of tool carrier machine for special applications such as maintenance of agricultural ponds and embankments.
Vegetable & fruit picking robots	Remote control of robots for fruit and vegetable picking during the harvest.

Table 8: Agriculture Use Cases

Airport Use Cases

Use Case	Description
Baggage tractor	Remote operation of tractor used for transport of luggage in the airside of the airports.
Snow clearance operations	Remote operation of snow clearance machines from the airport operation centre to remove snow from the runway.
Remote delivery of car upon arrival	Remote delivery of preferred car to the airport pickup area for rental purposes via a mobile application.
Transport shuttles	Remote driving of shuttles on the airside of the airport for passenger transport.
Indoor operation	Remote driving of robots from an operation centre for floor cleaning, waste disposal and passenger guidance activities.
Airside maintenance support	Teleoperated driving of vehicles or robots used for maintenance activities such as inspection, runway cleaning etc., in the airside of the airports.
Remote valet parking	Remote driving operator undertakes to park the vehicle, supported by real-time video streaming that is sent from remotely driven vehicle.
Platooning	Remote driving a group of vehicles from a pilot/escort vehicle where the pilot vehicle is driven by an Operator, and it functions as a teleop centre.

Table 9: Airport Use Cases

Mining Use Cases	
Use Case	Description
Remote driving of dozer, loader & excavator	Teleoperated driving of heavy earth moving machinery such as dozer, loader and excavator used in rough mining conditions.
Remote driving of haulage trucks	Teleoperated driving of trucks used to transport most common form of mining materials such as mineral-ore and waste in open-pit mines.
Remote driving in dangerous areas	Remote guidance of mining vehicle during difficult situations such as mine blasting, hazardous gaseous environments, heavy dust operations, etc.
Guided tele-operations (Automated Guided Vehicle AGV)	Similar to trains on a railroad track, the operator controls acceleration and braking of the vehicle on a preset route.
Guarded tele-operations/Geofencing	Enables geo-fencing within tele-op control, allows users to create drivable areas within the map, and prevents users from driving in unsafe areas.
Driver training	Use of tele-operation technology to train new drivers of heavy equipment mining vehicles.
Auto tramming	This function is used to automatically deploy vehicles from one location to another and then take tele-op control when doing technical work.

Table 10: Mining Use Cases

Logistic Use Cases	
Use Case	Description
Intralogistics in warehouses	Remote control of yard trucks to navigate between loading and unloading docks, identify, retrieve and move trailers in huge logistic yards.
Smart yard shifting	Shifting of truck trailers from one position to other in large logistic yards of warehouses or distribution centres.
Store hailing	Teleoperation of robomarts, which are purpose-built mobile vehicle stores for grocery shopping which allow consumers to pick and buy goods at home.
Logistics in factory premises	Remote driving of trucks or robotic platforms for inward & outward logistic operations in closed factory premises such as delivery of assembly parts.
Last mile delivery	Teleoperated driving of vehicles or robots especially for last mile delivery purposes such as food delivery, parcel delivery and grocery delivery.
First mile delivery	Teleoperated driving of vehicles or robots especially for first mile delivery purposes such as parcel pick-up or transport of goods to warehouses.
Chemical transport	Teleoperated driving of vehicles or robots especially for transport of dangerous chemical in industrial plants.
Fleet management	Centralized remote control of vehicle fleets, ranging from electric vehicles on university campuses to large-scale public transport systems, enabling efficient fleet operations.
Remote vehicle delivery/renting	Vehicles are delivered directly to customers for rental or sharing purposes, facilitated by remote control, enhancing convenience and operational flexibility.

Table 11: Logistic Use Cases

4.2 Remote Operation Level (ROL)

4.2.1 Overview

It is important to understand the different levels of driving automation and ToD. This section will first explain the classification of driving automation as defined by the ISO/SAE PAS 22736:2021 (see 7.2), as well as various systems for classifying ToD, and then define a Taxonomy based on the research conducted.

4.2.2 Taxonomy of Driving Automation According ISO/SAE PAS 22736

The ISO/SAE PAS 22736 [69] standard defines six levels of driving automation, from no automation (Level 0) to full automation (Level 5) - see details in chapter 7.2. These levels describe how well a vehicle can handle driving tasks and manage different driving conditions.

The main goal of this section is to explain classifications for ToD as developed by organizations like the 5GAA, BSI, and researchers such as Bogdoll et al., highlighting the roles and responsibilities of Remote Operators in different situations.

Innovative classification systems from DriveU.auto and Beti Hypervision were also examined. These systems offer detailed approaches focusing on the integration of remote operations into automated driving and provide a more nuanced understanding of the different aspects and levels of ToD, particularly in the context of non-human remote operators and advanced automated systems. This clear classification not only helps clarify the current state of driving automation but also sets the stage for future developments in automated and teleoperated vehicle systems. Through this discussion, the section aims to provide a basic understanding of how these systems interact and evolve.

4.2.3 Taxonomy of Teleoperated Driving

Different frameworks have been proposed to classify ToD, focusing on the degree of Remote Operator involvement.

- **5GAA Framework:**
 - Non-ToD: All tasks managed by onboard systems or drivers
 - Dispatch ToD: Remote operator handles strategic decisions
 - Indirect Control ToD: Remote operator assists in tactical decisions
 - Direct Control ToD: Remote operator can fully control the vehicle
- **T-Systems Classification:**
 - Similar to 5GAA but uses slightly different terminology [70]
- **BSI Classification:**
 - Remote Monitoring: Oversight without direct control
 - Remote Assistance: Providing guidance to the vehicle
 - Remote Driving: Full real-time control of the vehicle
- **Bogdoll et al. RHIS (Remote Human Input Systems) Levels:**
 - Levels range from 0 (remote monitoring) to 5 (remote assistance with authorisation), paralleling levels in terms of automation
- **DriveU.auto Framework:**
 - Six levels, from T0 (Direct Drive) to T5 (Supervise), focusing on the degree of control and interaction between the vehicle and the remote operator

- **Beti Hypervision Levels:**

- Levels from 0 (No Hypervision) to 5 (Full AI Hypervision), focusing on the extent of remote supervision and automation integration.

The ISO/SAE PAS 22736 [69] standard for driving automation is widely accepted, but there are various systems for classifying Remote Operation Levels to assist and control AVs from a Remote Operation System. These can be broadly divided into two categories: those that assess the immediacy of remote control (like 5GAA, BSI, and T-Systems) and those that focus on the interaction between the AV and remote operators (such as the systems proposed by Bogdoll et al. and DriveU.auto).

The classifications differ in their emphasis and application, with some being more tailored towards human or machine remote operators. The Beti system, for example, specifically addresses remote supervision, adding nuances to the Indirect Control ToD category.

4.2.4 Taxonomy for Remote Operation

Taxonomy, as applied in this report, refers to a structured classification system that organizes concepts or processes into defined categories or levels. It provides as a clear and consistent framework for analysing and distinguishing various Remote Operation Levels (ROLs) across different scenarios.

Using a systematic methodological approach, including insights from research projects, structured internal workshops, existing frameworks for ToD as discussed in chapter 4.2.3, the project team developed a tailored Taxonomy of Remote Operation Levels (ROLs) for the Remote Operation System (Figure 22).

The DriveU.auto framework was chosen as the foundation due to its simplicity and adaptability, and it was further refined to address the specific requirements of this project. The resulting Taxonomy for remote operation defines five distinct levels (ROL₁ to ROL₅), balancing comprehensiveness with practical applicability. Each level is characterized by specific technical and operational requirements, including sensor capabilities, communication robustness, and the degree of human interaction required. These requirements ensure safety and efficiency by clearly defining the responsibilities, tasks and roles of the Remote Operator within each ROL.

The following sections explain these ROL in detail, as they form the basis for establishing the Minimum Requirements.

4.2.4.1 ROL1 - Direct Control L1 – without OEDR sensors (Remote Driving)

This Use Cases of Remote Driving may occur in scenarios where Tele Driving is not possible, e.g. due to bad internet connections or poor visibility through the camera systems. In such situations, direct control ensures that the vehicle can still be operated safely despite the technological limitations (Figure 24).

The on-site Vehicle Driver directly controls the AV using on-site remote controller, relying entirely on their own skills to detect objects, plan routes, and manoeuvre the vehicle. This demands a high level of attentiveness and expertise, as there are no automated safety interventions to assist during the operation.



Figure 24: ROL1 - Representation of Direct Control without OEDR sensors

4.2.4.2 ROL2 - Direct Control L2 with OEDR sensors (Tele Driving)

This use cases may arise in situations where Teleassistance L1 is not possible, e.g. when the ADS is unable to drive automatically or when performing complex manoeuvres, such as safely putting the vehicle at the side of the road.

Here, the Remote Operator has full control of the AV in real-time, using live video feeds (Figure 25). They handle everything from planning the route to controlling speed and manoeuvring. The AV's sensors (OEDR) are active, adding an extra layer of safety by adjusting speed or braking in emergencies. This setup helps the Remote Operator make informed decisions with real-time data and sensor support.

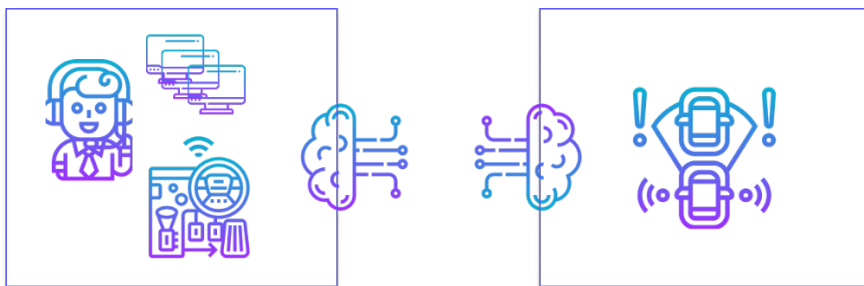


Figure 25: ROL2 - Representation of Direct Control with OEDR sensors

To enhance video stream robustness and network stability in a scenario where a Remote Operator controls an automated vehicle (AV) in real time, here are some examples of technical requirements to consider:

- **Guaranteed Low Latency:** Video streams must maintain latency below a critical threshold to allow timely operator responses
- **Consistent Frame Rate:** Video streams should provide a stable frame rate (e.g., 30 FPS or higher) to avoid jitter or visual artifacts that could hinder decision-making
- **Adaptive Resolution:** Implement adaptive video encoding (e.g., H.265 with variable bitrate) to adjust quality dynamically based on available bandwidth, ensuring uninterrupted streams
- **Error Detection and Correction:** Include Forward Error Correction (FEC) mechanisms to address packet loss, minimizing the impact of network disruptions
- **Optimized Compression:** Streams should be compressed to reduce bandwidth requirements while maintaining sufficient quality for critical details (e.g., road signs, pedestrian detection)
- **Minimum Guaranteed Bandwidth:** Allocate a minimum dedicated bandwidth to prevent interruptions or quality drops
- **Network Redundancy:** Utilize multiple communication channels to ensure continuity in case of a single network failure
- **QoS (Quality of Service):** Prioritize video streams and critical commands over the network to avoid interference from secondary tasks
- **Transmission Delay Management:** Implement protocols optimized for low-latency transmissions, such as QUIC or specialized TCP/IP versions
- **Real-Time Monitoring:** Deploy a monitoring system to detect and alert operators to network fluctuations or outages, enabling immediate corrective action

4.2.4.3 ROL3 and ROL4 - Indirect Control – Teleassistance Operation L1/L2

The Use Cases for Teleassistance Operation L1 (ROL3) arise when Teleassistance L2 (ROL4) is not possible, for instance, if the vehicle remains stationary for too long, requiring intervention to improve traffic flow or handle a priority agreement situation.

For Teleassistance Operation L2 (ROL4), the Use Cases include scenarios where the vehicle requires confirmation or a new path due to system limitations, obstructions on the driving path, vehicle uncertainty, or complex situations (Figure 26).

In these modes, the Remote Operator provides guidance or assistance rather than full control. The Remote Operator offers strategic advice, like suggesting alternate routes, without continuously managing the vehicle's speed or trajectory. This supports the AV's decision-making without taking over completely.

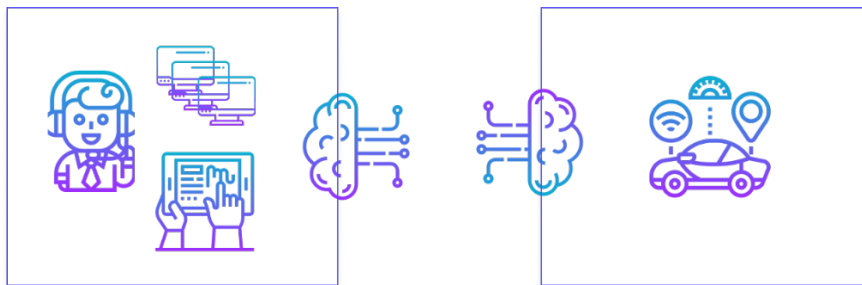


Figure 26: ROL3-4 - Representation of Indirect Control

For ROL3, the same technical requirements as for ROL2 should be considered, with additional emphasis on reliability and responsiveness. In this mode, the Remote Operator continues to play a crucial role in managing the vehicle's speed, which requires real-time access to accurate and stable information displayed at the Remote Operation Centre. Any latency, disruption, or degradation in the video streams or sensor data could significantly impact the Remote Operator's ability to make timely and informed decisions, increasing the risk of errors. Ensuring high-quality video feeds, robust network connectivity, and low-latency communication is therefore critical to maintaining operational efficiency and safety in ROL3 scenarios.

4.2.4.4 ROL5 - Monitoring

The Use Cases for Monitoring (ROL5) occur when the Automated Vehicle (AV) is operating under normal conditions and does not require active intervention from the Remote Operator. In this mode, the Remote Operator only has the task of monitoring the AV and ensuring that no problems occur. This role involves supervising system status, network integrity, and vehicle performance to maintain safety and operational reliability.

4.2.4.5 ROL overview table

The following Figure 27 (larger representation in chapter 7.3) illustrates the main characteristics of the different ROL levels which have been identified by the project team. These characteristics served as the foundation for developing specific requirements associated with each ROL. The categorization basis for ROL1 to ROL5 is defined according to the teleoperation Taxonomy established by DriveU.auto, as shown in Figure 9.

Driving automation level

It must be mentioned that a AV driving automation Level 4 or 5 according ISO/SAE PAS 22736, 2021 [69] is a prerequisite for a Remote Operation System such as the one under consideration here

Remote Operation Level	ROL 1	ROL 2	ROL 3	ROL 4	ROL 5
Designation	Remote Controller Driving	Tele Driving	Teleassistance Operation L1	Teleassistance Operation L2	Monitoring
Task	Full control of the vehicle Act like a normal driver Communication	Full control on the vehicle Act like a normal driver Communication	Path drawing Speed control Lights or other control Communication	Path drawing Path confirmation Communication	Supervision Communication
DDT responsibility of operator	Full	Full	Speed application	None	None
OEDR responsibility of operator	Full	None	None	None	None
Remote driver support system active	Collision Avoidance System AEBs*	Collision Avoidance System AEBs*	Vehicle fully automated	Vehicle fully automated	Vehicle fully automated
Responsibility	On-site Operator	Remote Operator	Automated Vehicle	Automated Vehicle	Automated Vehicle
Operator location	< 6 m	On the territory	On the territory	On the territory	On the territory
Speed limitation	6 km/h	6 km/h	Road limitation	Road limitation	Road limitation
Operational safety criteria (MRM trigger)	Remote controller communication	Video latency Driving data command latency	ADS operational Internet connection	ADS operational Internet connection	ADS operational Internet connection
Typical situation	Tele Driving not possible - Bad Internet connection - Bad visibility through camera	Teleassistance L1 not possible - ADS not able to drive autonomously - Complex manoeuvre (e.g. put vehicle at the side of the road)	Teleassistance L2 not possible - Vehicle stationary for too long - Improve traffic flow - Priority agreement situation	Vehicle need confirmation or new path - System limitation - Obstruction on the driving path - Vehicle uncertainty - Complex situation	- Automated Vehicle in normal operation - Part of troubleshooting procedure

*AEBs = Advanced Emergency Braking System
 *OEDR = Object and Event Detection and Response

Figure 27: Taxonomy of Remote Operation Levels (ROLs)

4.3 Scenarios

4.3.1 Introduction

Scenarios play a pivotal role in validating the functionality, safety, and adaptability of teleoperated systems in a variety of real-world contexts. They serve to identify critical challenges, guide the development of requirements, and provide a structured framework for testing and evaluation. By understanding these scenarios, it becomes possible to design a robust remote vehicle control and supervision system.

The development of representative scenarios followed a systematic approach that accounted for various influencing factors. These included vehicle dynamics, such as speed, manoeuvrability, and state, as well as external conditions like weather, road types, and traffic density. Internal workshops and expert interviews provided critical insights, ensuring that the scenarios captured diverse operational contexts and addressed key safety and performance considerations. Additionally, the process involved analysing Use Cases and conducting real-world testing in Switzerland. These steps emphasized the interaction between ADS and Remote Operators, capturing critical aspects of Teleoperation (ROL2) and providing a robust foundation for scenario design.

This section first explores the relevant Use Cases before presenting the defined Scenarios.

4.3.2 Use Cases

To establish specific requirements, the working group selected use cases from automated vehicle tests in Switzerland, including:

- **Last Mile automated delivery (LOXO):** Automated vehicles deliver goods within urban areas (Figure 28)
- **Last Mile Passenger Transportation (BFH):** Automated shuttles transport passengers in urban and private settings (Figure 29)
- **Automated Bus Depot (SwissMoves):** Automated buses operate within a depot, handling precise manoeuvres in a controlled space (Figure 30)

These use cases are relevant to Level 4 automated vehicles and provide insights from real-world tests. Factors like maximum speed (30-50 km/h), roadway types (urban, rural, parking, multi-lane), and specific intersections and signage were considered to define the ODD.

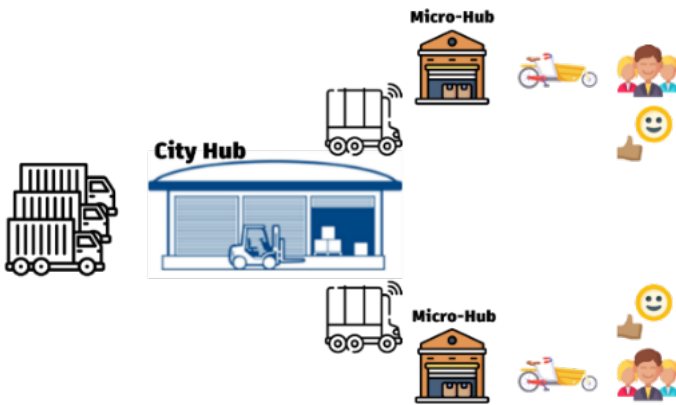


Figure 28: Automated Delivery on last mile Use Case (LOXO)

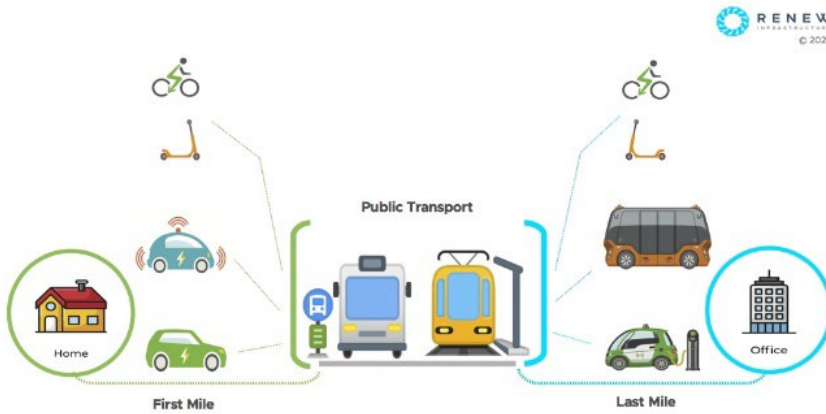


Figure 29: Last mile passenger transportation by automated shuttle Use Case (BFH)

Source : <https://renewinfra.com/>

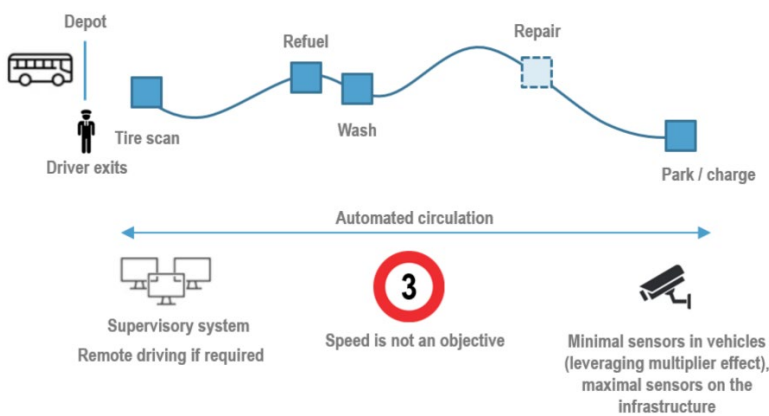


Figure 30: Automated bus depot Use Case (SwissMoves AutoDepot project)

Here is a typical ODD for these use cases:

- Maximum Speed: 30 km/h to 50 km/h (in automated mode)
- Roadway Types: Urban, rural, parking, multi-lane/single-lane roads, private roads, and pedestrian zones
- Intersection Types: Various, including stop signs, roundabouts, and crosswalks

- Signage: Traffic signals, stop/yield signs, and construction signage
- Roadway Users: Cars, buses, motorcycles, pedestrians, and others

4.3.3 Identification and description of relevant Scenarios

Relevant scenarios are identified based on real-world tests and existing literature. Each scenario is described functionally, encompassing potential sub-scenarios with similar events and solution routes. This approach focuses on solution strategies while keeping the number of scenarios manageable.

4.3.4 Selected Scenarios

The development of scenarios accounted for a wide range of factors to capture the diversity and complexity of real-world conditions. Key factors included weather conditions (e.g. rain, snow, fog, varying light levels), road conditions (e.g. surface types, layouts such as highways, urban streets, rural paths), and traffic density. These factors directly affect visibility, traction, sensor accuracy, and vehicle control. Temporary and permanent environmental obstacles (e.g. construction zones, debris, and movable objects), add complexity to object detection and avoidance. Reliable sensor data quality and stable real-time communication channels are crucial for accurate perception and control, particularly when considering the potential variability in network latency and data integrity. As detailed in chapter 3.1, the scenarios were also shaped by vehicle dynamics, such as speed, manoeuvrability, and state, which played a critical role in defining scenario viability and safety parameters. Informed by these factors, as well as insights from expert interviews and internal workshops, the project team selected eight representative scenarios for in-depth analysis. These scenarios, listed in Table 12 and illustrated in Figure 31, represent diverse operational contexts and address critical challenges in ensuring the reliability of Remote Operation Systems.

It is acknowledged, however, that the representativeness of these scenarios for all real-world operations, particularly in highly urbanized or remote rural environments, requires further investigation. While the selected scenarios reflect a broad range of operational contexts, additional testing in these specific settings would help validate their generalizability and identify potential gaps.

List of selected scenarios

Scenario	Description
Scenario 1	Unexpected road blockage
Scenario 2	Loss of network connectivity or poor network performance
Scenario 3	Imprecise location due to location system issue or signal loss
Scenario 4	Malfunction of optical sensor due to solar radiation
Scenario 5	GNSS and odometer give ambiguous results due to slippery road
Scenario 6	Adverse weather conditions
Scenario 7	Bottleneck in dense traffic
Scenario 8	False positive obstacle detection

Table 12 : List of selected scenarios

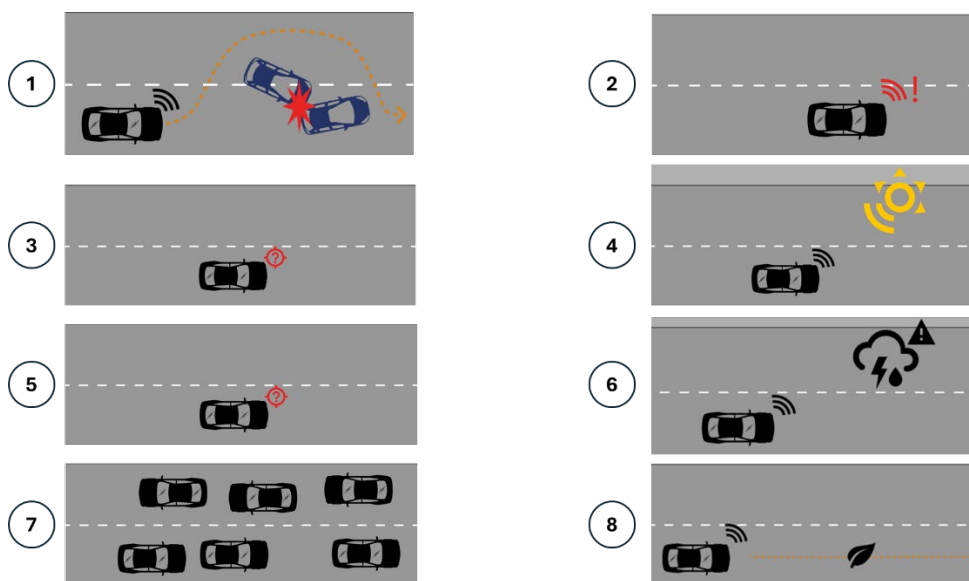


Figure 31: Overview of selected scenarios

Relevant scenarios are identified based on real-world tests and existing literature. Each scenario is described functionally, encompassing potential sub-scenarios with similar events and solution routes. This approach focuses on solution strategies while keeping the number of scenarios manageable.

Each scenario description includes **three phases**:

- **Phase 1: Problem Description** – Outlining the general configuration, including the environment and actors
- **Phase 2: Problem Detection** – Detailing the sequence of events leading up to the problem identification and decision for solution
- **Phase 3: Solution based on Remote Operation levels (ROL)** – Discussing possible solutions, criteria for applying them, and the roles of the remote operator and ADS

4.3.4.1 Scenario 1: unexpected road blockage

- Phase 1: An urban road is blocked by a stalled vehicle or construction site
- Phase 2: The automated vehicle detects the obstacle and stops, contacting the remote operator
- Phase 3: Depending on the road geometry and traffic conditions, the remote operator may reroute the vehicle or manually navigate it past the blockage

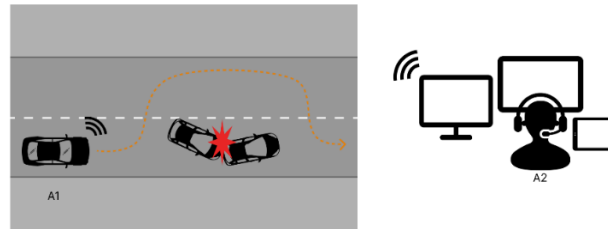


Figure 32: Scenario 1 - Representation of unexpected road blockage

4 - Tele Assistance Operation L2

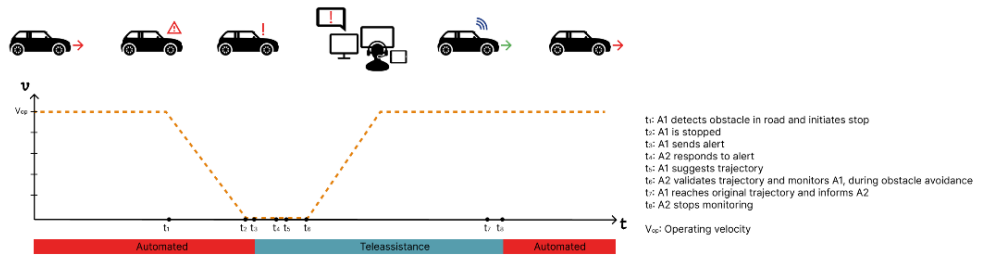


Figure 33: Scenario 1 - Unexpected road blockage resolution using ROL4

3 - Tele Assistance Operation L1

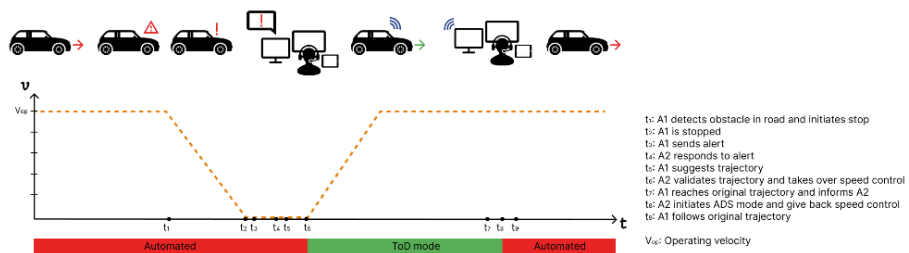


Figure 34: Scenario 1 - Unexpected road blockage resolution using ROL3

2 - Tele Driving

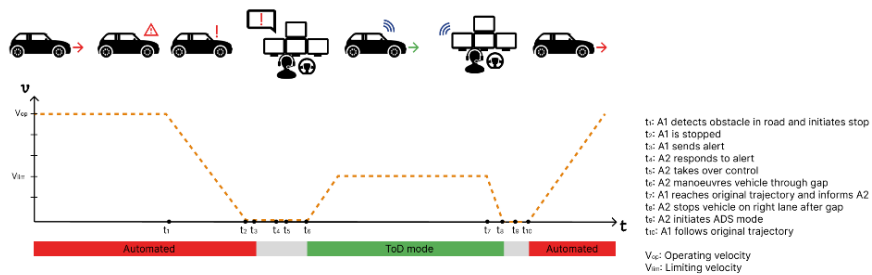


Figure 35: Scenario 1 - Unexpected road blockage resolution using ROL2

4.3.4.2 Scenario 2: loss of network connectivity or poor network performance

- Phase 1: The vehicle experiences degraded network performance
- Phase 2: The vehicle initiates MRM and contacts the Remote Operator
- Phase 3: If connectivity can be re-established, the vehicle continues under remote guidance; otherwise, on-site assistance is required

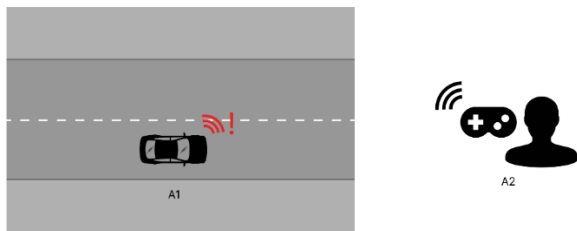


Figure 36: Scenario 2 - Representation of loss of network

1 - Remote Controller Driving

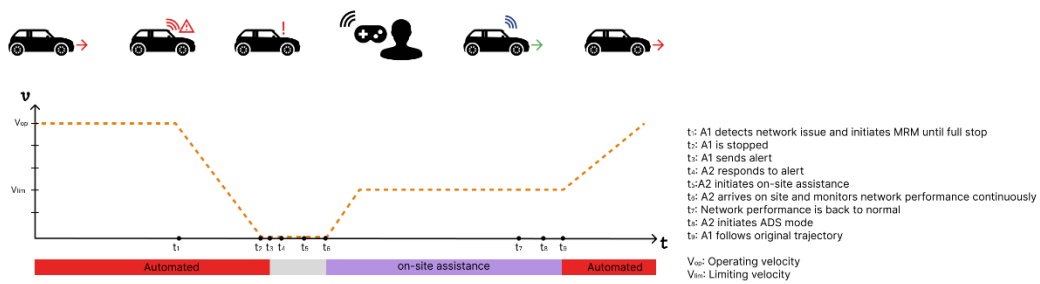


Figure 37: Scenario 2 - Loss of network resolution using ROL1

4.3.4.3 Scenario 3: imprecise location due to system issues

- Phase 1: Global Navigation Satellite System (GNSS) or other location systems fail due to environmental factors
- Phase 2: The vehicle detects the issue and contacts the remote operator
- Phase 3: The remote operator may manually navigate the vehicle if conditions allow or request on-site assistance

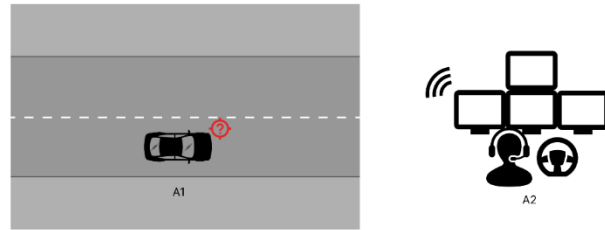


Figure 38: Scenario 3 - Representation of imprecise location

2 - Tele Driving

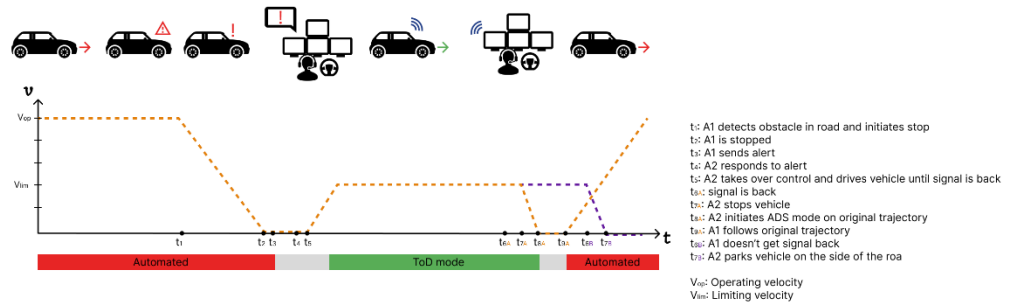


Figure 39: Scenario 3 - Imprecise location resolution using ROL2

4.3.4.4 Scenario 4: malfunction of optical sensors due to solar radiation

- Phase 1: Sunlight interferes with the vehicle's sensors
- Phase 2: The vehicle stops and contacts the remote operator
- Phase 3: The remote operator may manually drive the vehicle to a safer location with better sensor performance

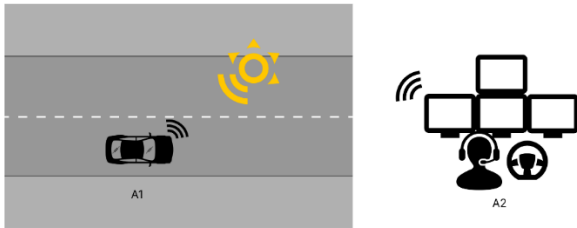


Figure 40: Scenario 4 - Representation of solar radiation

2 - Tele Driving

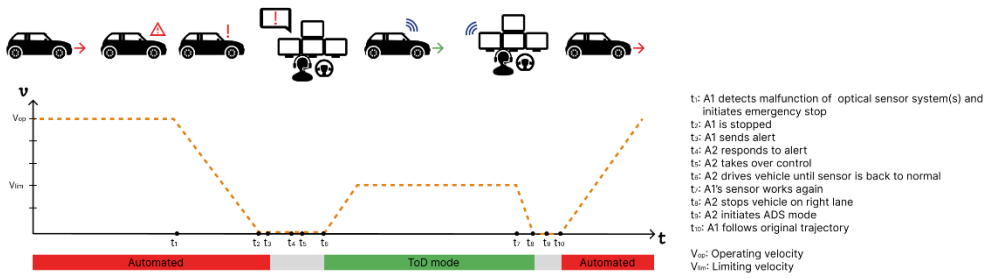


Figure 41: Scenario 4 - Solar radiation resolution using ROL2

1 - Remote Controller Driving

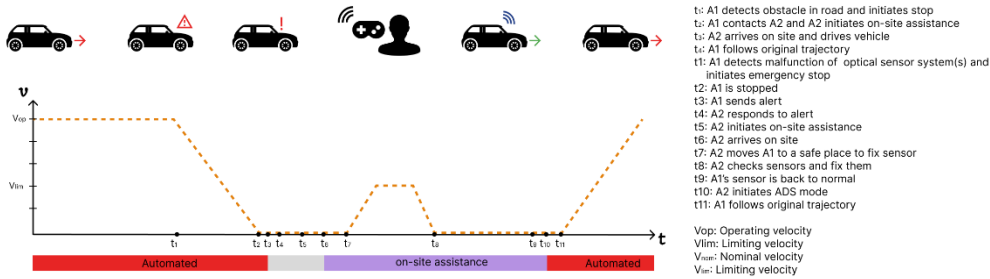


Figure 42: Scenario 4 - Solar radiation resolution using ROL1

4.3.4.5 Scenario 5: GNSS and odometer give ambiguous results due to slippery road

- Phase 1: The vehicle encounters a slippery road, causing GNSS or odometer inaccuracies
- Phase 2: The vehicle detects the issue and contacts the remote operator
- Phase 3: The operator assesses whether manual driving is possible or if on-site assistance is necessary

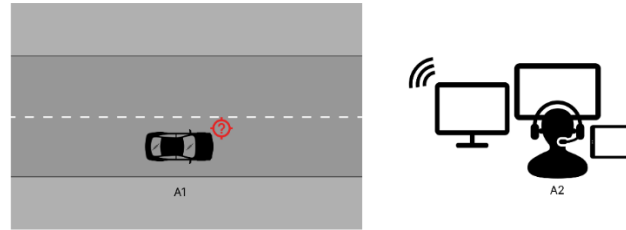


Figure 43: Scenario 5 - Representation of ambiguous sensor results

4 - Tele Assistance Operation L2

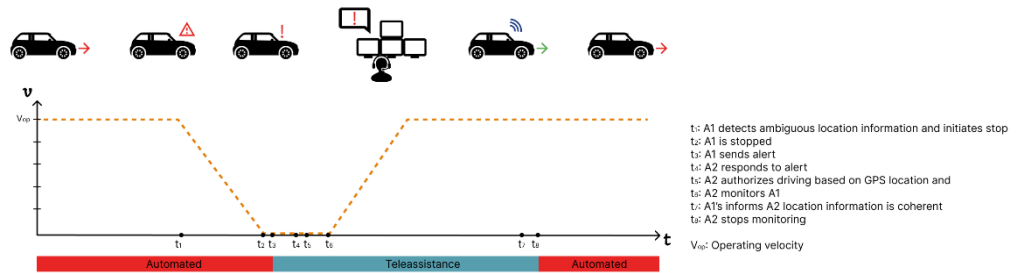


Figure 44: Scenario 5 - Ambiguous sensor results resolution using ROL4

3 - Tele Assistance Operation L1

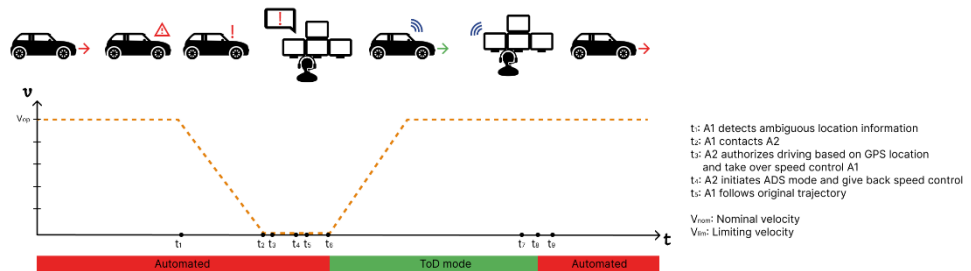


Figure 45: Scenario 5 - Ambiguous sensor results resolution using ROL3

4.3.4.6 Scenario 6: adverse weather conditions

- Phase 1: Poor visibility due to weather conditions like rain or fog
- Phase 2: The vehicle detects visibility issues and contacts the remote operator
- Phase 3: Depending on visibility, the remote operator may either continue remotely or arrange for on-site assistance

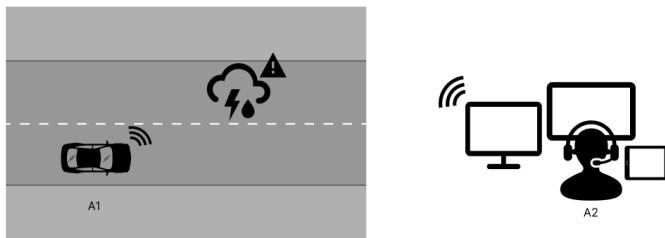


Figure 46: Scenario 6 – Representation of adverse weather conditions

3 - Tele Assistance Operation L1

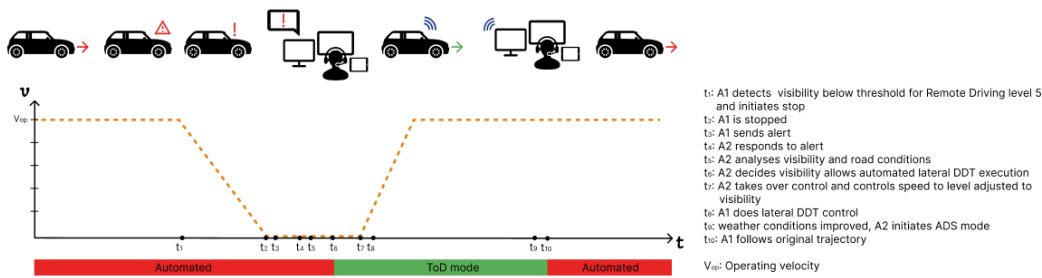


Figure 47: Scenario 6 - Adverse weather conditions resolution using ROL3

2 - Tele Driving

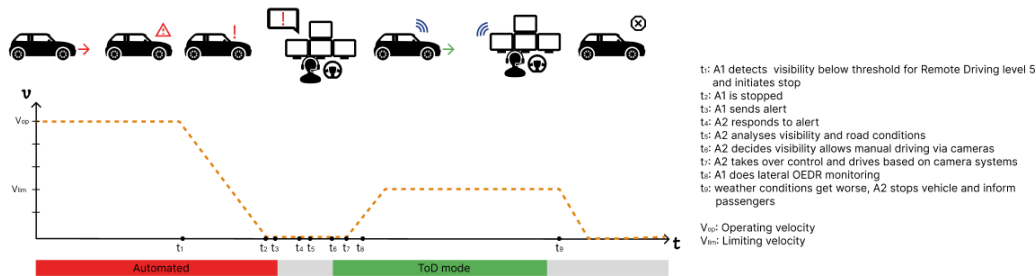


Figure 48: Scenario 6 - Adverse weather conditions resolution using ROL2

1 - Remote Controller Driving

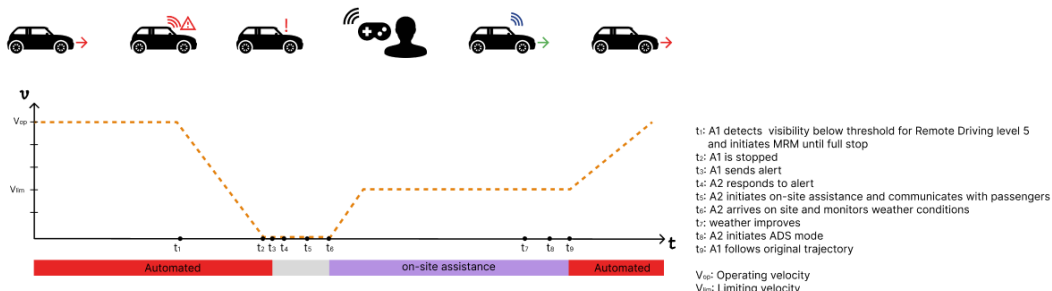


Figure 49: Scenario 6 - Adverse weather conditions resolution using ROL1

4.3.4.7 Scenario 7: bottleneck in dense traffic

- Phase 1: The vehicle approaches a bottleneck with heavy oncoming traffic
- Phase 2: The vehicle stops and requests assistance
- Phase 3: The remote operator may communicate with other vehicles to navigate through the bottleneck or request on-site help

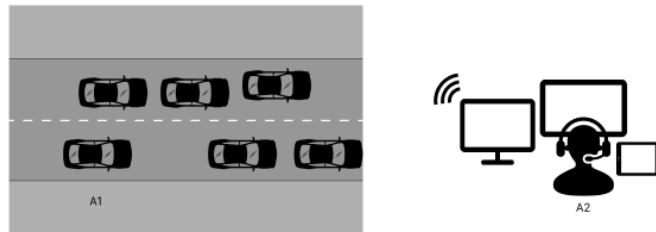


Figure 50: Scenario 7 – Representation of bottleneck in dense traffic

4 - Tele Assistance Operation L2

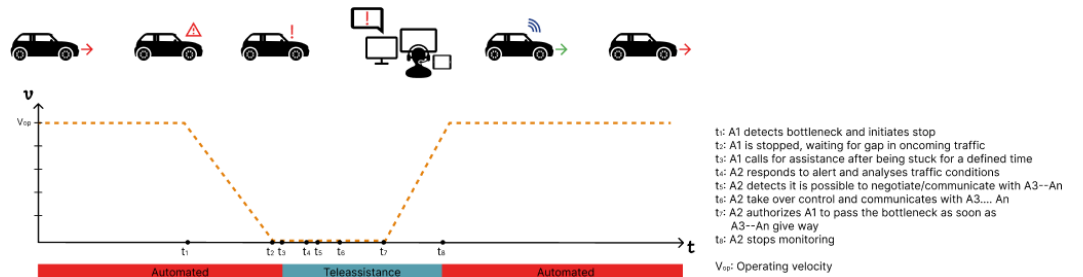


Figure 51: Scenario 7 - Bottleneck in dense traffic resolution using ROL4

3 - Tele Assistance Operation L1

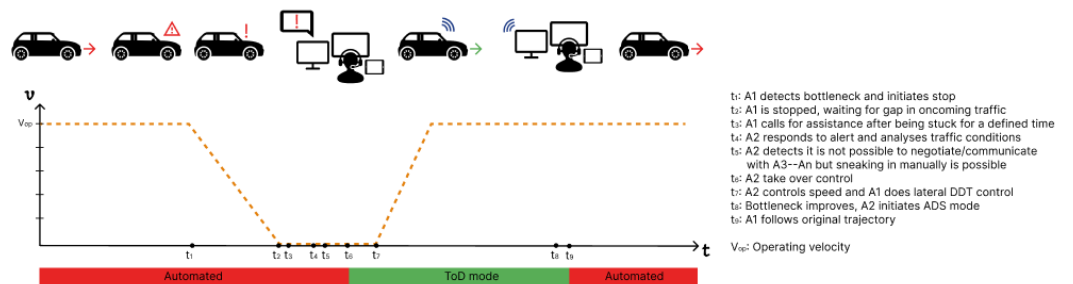


Figure 52: Scenario 7 - Bottleneck in dense traffic resolution using ROL3

2 - Tele Driving

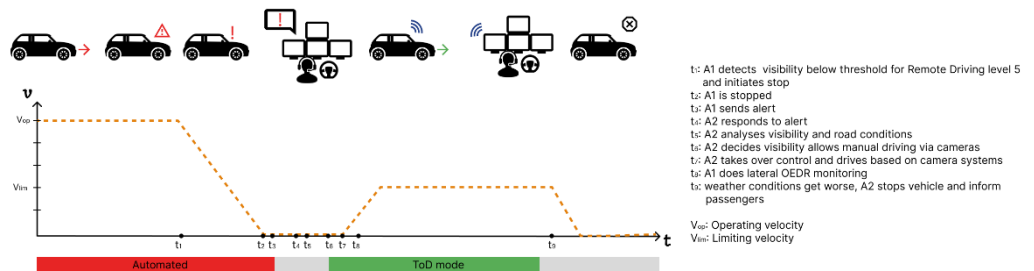
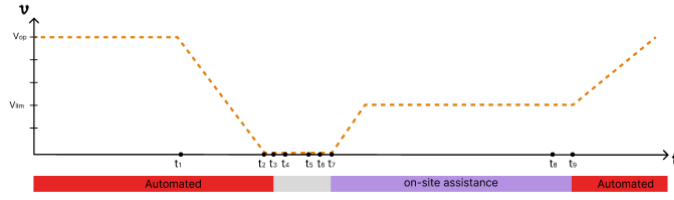


Figure 53: Scenario 7 - Bottleneck in dense traffic resolution using ROL2

1 - Remote Controller Driving



- t₁: A1 detects bottleneck and initiates stop
- t₂: A1 is stopped, waiting for gap in oncoming traffic
- t₃: A1 calls for assistance after being stuck for a defined time
- t₄: A2 responds to alert and analyses traffic conditions
- t₅: A2 initiates on-site assistance and communicates with passengers
- t₆: A2 arrives on site and stops oncoming traffic
- t₇: A2 does remote driving Level 4 through gap
- t₈: Once past the bottleneck, A2 initiates ADS mode
- t₉: A1 follows original trajectory

V_{op} : Operating velocity
 V_{lim} : Limiting velocity

Figure 54: Scenario 7 - Bottleneck in dense traffic resolution using ROL1

4.3.4.8 Scenario 8: false positive obstacle detection

- Phase 1: The vehicle detects a false obstacle, such as leaves or debris
- Phase 2: The vehicle stops and contacts the remote operator
- Phase 3: The operator decides whether to avoid the obstacle or proceed cautiously if avoidance is not possible

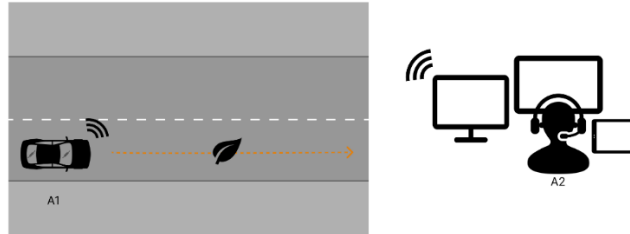


Figure 55: Scenario 8 - Representation of false positive obstacle detection

4 - Tele Assistance Operation L2

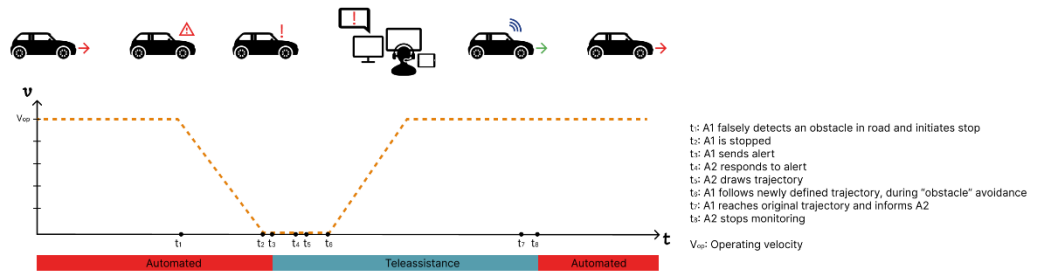


Figure 56: Scenario 8 - False positive obstacle detection resolution using ROL4

3 - Tele Assistance Operation L1

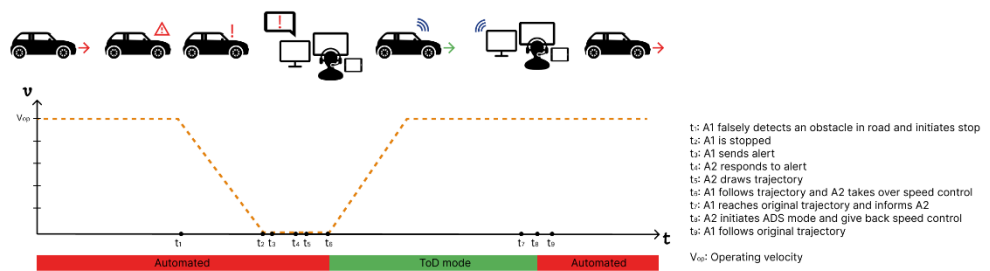


Figure 57: Scenario 8 - False positive obstacle detection resolution using ROL3

2 - Tele Driving

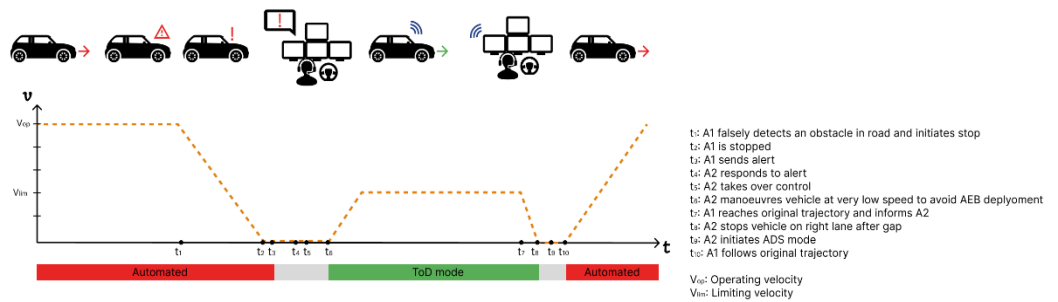


Figure 58: Scenario 8 - False positive obstacle detection resolution using ROL2

4.4 Definition of Requirements

4.4.1 Overview

Defining clear and comprehensive requirements is a critical step in ensuring the successful implementation and operation of remotely driven AVs. This section outlines the specific requirements identified during this research project, focusing on technical specifications, safety protocols, and operational guidelines. The requirements were developed through a systematic, multi-step approach, incorporating a thorough analysis of international standards, real-world testing, and expert input. This ensures their practical applicability, scalability, and alignment with operational safety standards while addressing the dynamic challenges of remote operation technology.

4.4.2 Requirement Definition

To establish the requirements, the working group created a template to clearly identify each requirement. This process drew on experience from previous projects, expert workshops and established standards such as ISO 26262, ISO 21434, ISO 13849, and ISO 61508. The following principles must be considered when defining requirements:

- Avoiding ambiguity:
 - The car shall be blue → What does blue mean?
 - The car shall be sky blue [#7BAFD4]
 - Use a good verb, prefer the form « shall »
- Avoid unclear adverbs:
 - The system shall reasonably ...
 - The system shall work as fast as possible ...
 - The system shall significantly improve ...
 - → Measurable? Verifiable? Testable?
- Avoid negations:
 - The system shall not provide not more than 4MB → NOK
 - The system shall provide more than 4MB → OK
- Atomic:
 - A requirement includes a single need
- Complete:
 - Avoid abstractions « it makes sense that ... »
- Consistent:
 - Avoiding conflicting ideas or contradictions
- Non-redundant
- Implementable

Figure 59 represents the form a requirement must take.

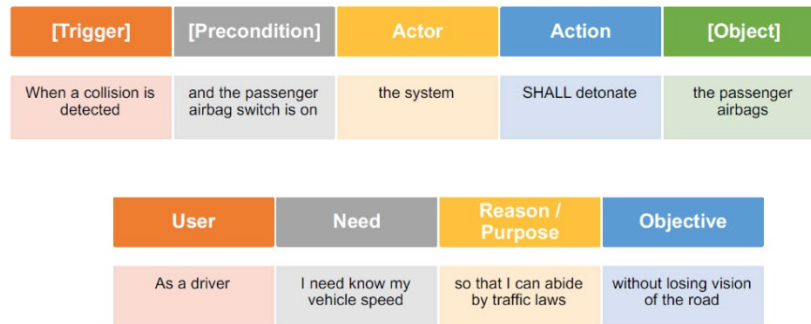


Figure 59: Form of requirements

Table 13 provides detailed explanations of each column and its associated categories.

Description of requirement definitions

Column name	Description
ID	A unique identifier (ID) is a unique alphanumeric code assigned to a specific requirement within a project. Its primary purpose is to facilitate clear communication, tracking, and management of requirements throughout the development process. Each ID is associated with a detailed description of the requirement, allowing stakeholders to easily reference and verify specific criteria. By using IDs, teams can ensure that all requirements are accounted for and addressed systematically, minimizing the risk of confusion or oversight during implementation and testing.
Category	<p>Remote Vehicle</p> <p>The "Remote Vehicle" category encompasses essential elements required for its operation. Key requirements include basic functionality, which ensures the vehicle meets necessary standards. Actuators, such as steering and braking systems, are critical for precise control and manoeuvrability. The command interface and execution facilitate seamless interaction with the vehicle, allowing for effective remote operation. Additionally, the interface with sensors is crucial for real-time data collection and feedback, enhancing the vehicle's performance and safety.</p> <p>Remote Operator Station</p> <p>The "Remote Operator Station" category includes vital components necessary for effective remote vehicle operation. Key infrastructure and materials are essential for building a reliable station. Driving commands, encompassing steering and braking, ensure precise control of the vehicle. The station's location is crucial for optimizing operational effectiveness and maintaining a clear line of sight. Additionally, the Human-Machine Interface facilitates user interaction, providing operators with intuitive controls and real-time feedback for enhanced situational awareness and decision-making.</p> <p>Remote Operator</p> <p>The "Remote Operator" category outlines the essential skills and prerequisites required for effectively operating an automated vehicle from a distance. It encompasses</p>

Column name	Description
	<p>the minimum competency requirements, along with crucial information needed for safe and efficient remote driving. This includes training on the Remote Operation System, knowledge of the automated vehicle, a checklist for operations, and emergency contact protocols.</p>
	<p>Communication</p> <p>The "Communication" category outlines the essential requirements for ensuring secure data exchange between systems. It defines the necessary security measures to prevent unauthorized access and protect against the transmission of fraudulent messages. Additionally, it establishes the restrictions and protocols that must be implemented based on the vehicle's speed and data transmission latency, ensuring reliable and timely communication essential for safe operation.</p>
Req. Type	<p>Functional</p> <p>Functional requirements describe the functions and features that the system must provide. They outline what the system should do to meet user needs. For example, a functional requirement for a Remote Operation System for automated vehicles could be "The system must allow the user to remotely control the speed and direction of the vehicle."</p> <hr/> <p>Performance</p> <p>Performance requirements specify the performance levels that the system must achieve to operate effectively. They define performance criteria such as speed, accuracy, reliability, etc. For example, a performance requirement for the Remote Operation System could be "The system must allow for a maximum data transmission latency of less than xxx milliseconds."</p> <hr/> <p>Design</p> <p>Design requirements describe the design constraints and specifications that the system must adhere to. They may include considerations such as size, weight, power consumption, ease of use, etc. For example, a design requirement for the system could be "The Teleoperation device must be portable and easy to handle."</p> <hr/> <p>Environment</p> <p>Environmental requirements define the environmental conditions under which the system must operate. They include factors such as temperature, humidity, vibrations, shocks, etc. For example, an environmental requirement could be "The system must operate reliably in temperature conditions ranging from -20 °C to 50 °C."</p> <hr/> <p>Operational</p> <p>Operational requirements describe the procedures and operations that users must follow to use the system correctly. They include usage instructions, safety protocols, startup/shutdown procedures, etc. For example, an operational requirement could be "Users must undergo a two-hour training on using the system before operating it."</p> <hr/> <p>Interface</p> <p>Interface requirements define the interactions between the system and users or other systems. They specify data formats, communication protocols, user interfaces, etc. For example, an interface requirement could be "The system must be compatible with standard communication protocols used by automated vehicles to enable seamless integration."</p>

Column name	Description
ROL	Link between the requirement and the Remote Operation Level, as a reminder: <ul style="list-style-type: none"> • ROL1 : Remote Driving • ROL2 : Teleoperation • ROL3 : Teleassistance Operation L1 • ROL4 : Teleassistance Operation L2 • ROL5 : Monitoring
Requirement Description	Description of the requirement respecting the form described in Figure 59
Remarks	Additional information to the requirement description
Source	<p>Norm Standards set by standardization bodies or governmental regulations</p> <hr/> <p>Studies Conclusions drawn from relevant research or analysis</p> <hr/> <p>Own experience Insights based on past experiences</p> <hr/> <p>Estimations Forecasts based on models or expert knowledge</p> <hr/> <p>Not yet defined Source for the requirement not yet specified or determined</p>
Source Spec.	Additional information to specify the source (location, standard/regulation name, paper, etc.)

Table 13: Description of requirement definitions

4.4.3 Requirement Categories

The minimum requirements were developed based on the practical experience at LOXO, the outcomes of various projects carried out by the HEIA-FR, ROSAS, SwissMoves, and BFH, and the information available in OCA/VAF and the EU (Figure 60).

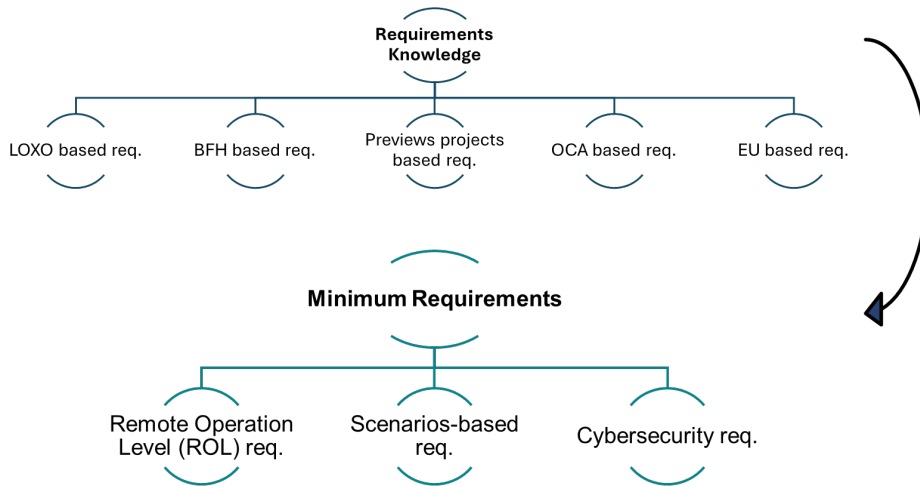


Figure 60: Derivation of the minimum requirements

To make the requirements clearer, the working group categorized them into three main types. This division helps provide a better understanding of the different requirements. The three main categories are as follows:

- 1. Requirements for Remote Operation Level (ID for requirements RROLxxx):** This section outlines the requirements for various levels of remote operation, as defined in section 4.2 *Remote Operation Level (ROL)*. It serves to identify the minimum safety standards necessary for each ROL to ensure the secure operation of the automated vehicle. Notably, ROL 1 is excluded from these requirements, as it pertains to on-site control of the vehicle via a remote control, rather than remote operation without visual contact.
- 2. Requirements for Scenario-Based Operations (ID for requirements RSBxxx):** These requirements are defined based on the critical scenarios identified. The various scenarios are described in section 4.3.4. Indeed, the analysis of these scenarios has allowed for the identification of risks or issues that necessitate specific safety measures and operational guidelines to ensure effective risk management and the safe functioning of the automated vehicle.
- 3. Cybersecurity Requirements (ID for requirements CRxxx):** Requirements defined for cybersecurity aspects to protect automated vehicles, communication and the remote operations centre.

4.4.4 Elaboration of the Requirements

To establish these minimum requirements, the working group undertook several iterative steps, resulting in a refined set of requirements.

1. Initial Database

Technical requirements were gathered from previous projects conducted by HEIA-FR (ROSAS/SwissMoves) and BFH, as well as approximately 1,000 internally developed requirements provided by LOXO and BFH for validation of automated vehicles and remote operation technology. A preliminary screening was performed to retain only requirements relevant to the project's objectives and the following categories: Remote Vehicle, Remote Operator Station, Remote Operator, and Communication (see Figure 3).

2. Analysis of Standards

An extensive review of national and international standards was conducted. Notable frameworks include UN Regulation No. 46 and ISO 16505:2019 (including Amendment 1:2021), which provide critical guidelines for camera-monitor systems (CMS). These standards ensure reliable visibility and operational safety under diverse conditions. Aligning the project's defined requirements with these international standards strengthens their scalability and provides a robust foundation for future regulatory approval processes.

3. Categorization by ROLs

Since various modes of remote operation exist (direct control or indirect control), requirements were categorized based on the Remote Operation Levels (ROLs) defined in Section 4.2. Each requirement was associated with one or more ROLs, ensuring applicability across different operational contexts.

4. Use Cases and Scenarios

Complementary to the initial screening, Use Cases and Scenarios were defined to clarify the scope of remote operation. These scenarios informed the creation of a new, more general list of requirements.

5. Iterative Refinement

Following stakeholder reviews, the working group refined the requirements to address practical implementation challenges while ensuring they remain verifiable by regulatory bodies.

The details of the identified minimum requirements are presented in 7.1 A1 - List of Minimum Requirements. Figure 61 below gives an overview of the number of requirements and their distribution according to the 3 categories defined above:



Figure 61: Overview of identified minimum requirements

Here are a few examples for each of the 3 categories:

Remote Operator requirements (examples)						
ID	Category	Req. Type	ROL	Description	Source	Source Spec.
RROLo60	Remote Operator	Operational	ROL2, ROL3, ROL4, ROL5	The Remote Operator shall be located within Swiss territory.	Norm	OCA Art.33 (1)
RROLo70	Remote Vehicle	Operational	ROL2	During ROL2, the maximum speed of the Remote Vehicle shall not exceed 6 km/h.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L221/18 Art. 10
RROLo80	Communication	Performance	ROL2	During ROL2, the roundtrip latency (from AV camera to remote operation centre and from remote operation centre to AV actuators) shall be less than 850 ms.	Own experience	Confirmed by tests done at DTC
RROLo90	Remote Vehicle	Operational	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall undergo a daily routine remote driving check before it operates.	Norm	OCA Art.32 (2)

Table 14: Remote Operator requirements (examples)

Remote Vehicle requirements (examples)						
ID	Cate- gory	Req. Type	ROL	Description	Source	Source Spec.
RSB010	Re- mote Vehi- cle	Func- tional	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall be able to send, receive, check and display data from and to the Remote Operator Station.	Own experi- ence	
RSB210	Re- mote Vehi- cle	Func- tional	ROL2	The Remote Vehicle shall indicate whether it is currently in remote operating mode.	Norm	COMMISSION IM- PLEMENTING REGULATION (EU) 2022/1426 L 221/32 Art. 3.5.3.1
RSB240	Re- mote Oper- ator Sta- tion	Func- tional	ROL2	The Remote Operator Station shall receive visual and audio alerts in critical cases.	Own experi- ence	Critical cases: -Failure alerts - Automated emer- gency braking (AEB) triggered or alerts -Network alerts -Changing vehicle driving mode alerts

Table 15: Remote Vehicle Requirements (examples)

Communication requirements (examples)						
ID	Cat- e- gory	Req. Type	ROL	Description	Source	Source Spec.
CR0010	Com- mu- nica- tion	Cy- berse- curity	ROL2, ROL3, ROL4, ROL5	The communication between the vehicle and the TCC shall be authenticated.	Norm	UN ECE R155, An- nex 5
CR0290	Com- mu- nica- tion	Cy- berse- curity	ROL2, ROL3, ROL4, ROL5	Malware which can be trans- mitted during communica- tion shall be detected.	Norm	ISO 27001:2022, 5.14, IKT (Informations- und Kommunikati- onstechnik) DE.CM-4
CR1690	Re- mote Vehi- cle	Cy- berse- curity	ROL2, ROL3, ROL4, ROL5	The software update shall be installed when the vehicle is in a safe and secure state.	Norm	UN ECE R156

Table 16: Communication requirements (examples)

4.4.5 Cybersecurity Requirements

This section provides a detailed overview of the methodology employed to delineate the cybersecurity requirements. A formal risk assessment would be the best approach to define high-level requirements. However, due to time constraints and the desire to remain more technology-agnostic, the research team decided to use existing cybersecurity controls catalogues. Therefore, the requirements listed in this document represent only a baseline, similar to the threat catalogue mentioned in UN ECE R155 for vehicles. A comprehensive list of these requirements is available in Annex 7.1. The methodology encompasses the following steps.

- **Definition of the system under consideration:** This initial step involves a thorough description of the system being analysed to establish a clear context for the cybersecurity requirements.
- **Definition of sources of information:** This step entails identifying and documenting the various sources of information that will be utilized to gather relevant data on cybersecurity needs.
- **Refinement of cybersecurity requirements:** In this final step, the preliminary cybersecurity requirements are refined and elaborated to ensure they meet the necessary standards and are tailored to the specific needs of the system under consideration.

4.4.5.1 Definition of the system under consideration

The entire remote driving system has been evaluated to derive cybersecurity requirements. Adopting the same methodology used for deriving functional requirements, the system as shown in Figure 62 is systematically divided into four primary components:

- Remote Operator Station
- Remote Vehicle (Automated Vehicle)
- Communication
- Remote Operator

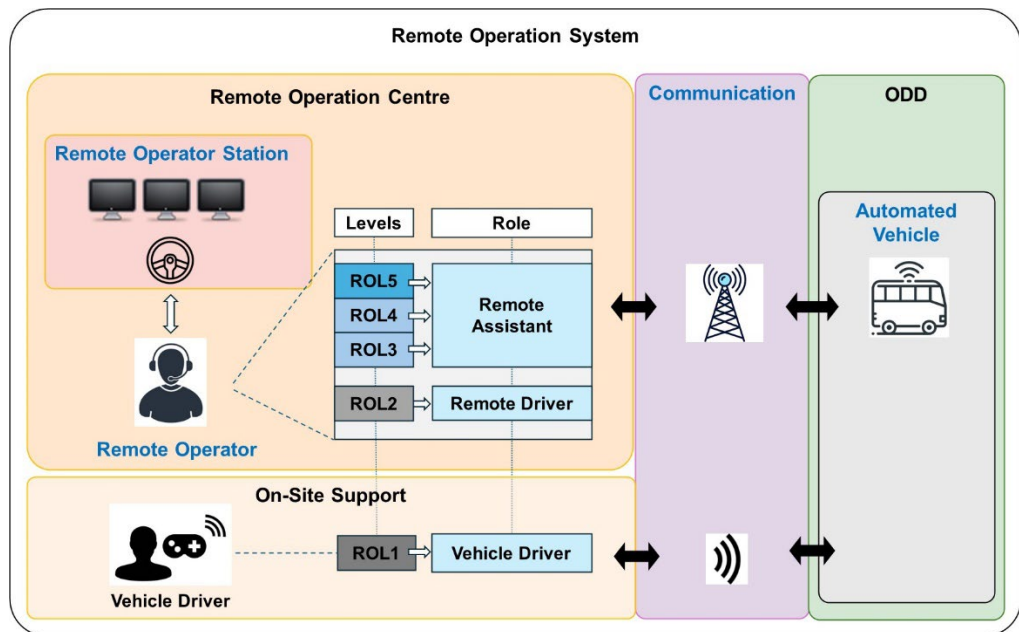


Figure 62: Cybersecurity-relevant elements of the Remote Operation System (blue)

4.4.5.2 Definition of sources of information

Cybersecurity requirements are derived from existing regulations, technical standards, and common knowledge. This approach facilitated the research group's task of defining the cybersecurity requirements without the need for formal, exhaustive cybersecurity risk assessments for all systems under consideration. In addition to UN Regulation No. 155 (Cybersecurity and Cybersecurity Management System) and ISO/IEC 27001:2024 (Information Security, Cybersecurity, and Privacy Protection),-which are elaborated in Chapters 2.4 resp. in 2.5, the following sources were also utilized:

- **ISA (International Society of Automation)/IEC 62443:** This family of Operational Technology (OT) cybersecurity standards is recognized as the equivalent of the ISO/IEC 2700x series for the OT environment. Compliance with parts of this standard can help meet new European regulations such as the Cyber Resilience Act (CRA) and the Network and Information Systems Directive (NIS2)
- **Information and Communications Technology (ICT) Minimum Standard:** Developed by the Federal Office for National Economic Supply (FONES) in collaboration with external cybersecurity experts, this standard is primarily based on existing standards like ISO/IEC 27001, National Institute of Standards and Technology (NIST) 800-53, and ISA/IEC 62443
- **General Data Protection Regulation (GDPR)/LPD (Loi sur la protection des données):** Data privacy considerations were also included to derive cybersecurity requirements, ensuring the protection of Personally Identifiable Information (PII)

4.4.5.3 Refinement of cybersecurity requirements

Each requirement is assigned to a specific system under consideration (see 4.4.5.1). This assignment enables stakeholders to select applicable requirements relevant to their systems. For ease of reference, the source of each requirement is mentioned, allowing stakeholders to gather more detailed information easily.

Additionally, each requirement includes a remote operation level designation. Some requirements are accompanied by additional remarks to provide further explanation or to tailor the requirements to specific use cases.

4.4.6 Summary

Finally, all requirements were compiled and organized to produce a final version containing the minimum requirements suggested by the working group. These requirements, presented in *7.1 A1 - List of Minimum Requirements*, reflect a comprehensive approach to addressing operational, safety, and cybersecurity challenges.

The most complex requirements are those related to the minimum data transmission latencies necessary for safely operating or monitoring an AV remotely. Further research, including tests across various scenarios, would be needed to refine the latencies established in this project.

4.5 Requirements Validation

4.5.1 Introduction

Within the present project, a set of minimal requirements for Teleoperation (ROL2) has been proposed. The “validation” of any of these requirements is defined as a check that (i) the proposed requirement addresses a relevant problem, (ii) that the proposed numerical values of physical quantities are sufficient and can realistically be achieved and that (iii) the requirement is in accordance with existing regulations or norms if applicable.

The validation according to this definition ensures that the proposed minimal requirements are necessary for the safe operation of teleoperated vehicles, and that each requirement is sufficiently strict. What cannot be validated in this way is the completeness of the proposed set of requirements (i.e. that no necessary requirement of a safe operation is missing). Therefore, the completeness of the set must be checked according to the list of relevant scenarios, which was done in WP 2. Finally, the proposed list of requirements must be seen as an initial proposal of a dynamic list which continuously has to be updated according to the available field data.

4.5.2 Scenarios and List of Requirements

The core output of WP2 was the list of minimal requirements for Teleoperation (ROL2). The requirements are based on existing literature, established standards, insights from expert interviews, and the consortium's experiences from initial tests with ToD during and before the project. They are formulated as functional, operational, performance and cybersecurity requirements and cover all relevant aspects of ToD (AV, Remote Control System, camera monitoring system, etc.). The list of requirements is a separate deliverable of the project which is available in annex 7.1.

As a foundation for the development of minimal requirements, a list of relevant scenarios for ToD has been defined. The selection was based on scientific literature, expert interviews (see chapter 3.1), and prior experiences and tests conducted by the consortium. These scenarios represent the most relevant problems with teleoperated vehicles operating on public roads. Apart from the scenario descriptions, they also contain proposed solution routes in terms of remote operation levels (ROLs). The scenario descriptions are to be understood as generalized descriptions on the “functional” level according to ISO 34501:2022 [71]. As such, each contains several possible sub-scenarios with slightly different scenery, detailed configuration of actors, dynamic/static entities, but a similar chain of events and the same applicable solution routes. The detailed list of scenarios can be found in section 4.3.4.

4.5.3 Validation Methods

In this section, the validation methods and their application to the different types of requirements will be presented. Please note that the cybersecurity requirements are discussed in a dedicated section (4.5.6).

4.5.3.1 Application or modification of existing regulations and norms

Many aspects of ToD are directly or indirectly covered by existing regulations and norms. In order to be consistent with the current industry standards and conventions, the proposed requirements follow these existing standards as closely as possible, even in cases where they are not mandatory under Swiss law. In some cases, the existing standards can directly be applied, in other cases (where they are not intended for this exact application), a slight adaptation to the context of ToD is necessary. Consequently, the validation of these requirements consists mainly in checking that the formulations are harmonised with the existing standards and that the sources are attributed correctly. This validation method is applicable for all kinds of requirements, but often less useful with performance requirements, as the specified performance values might require additional validation to ensure their validity when applied to ToD (see section 4.5.3.3).

The sources used for this validation route include the following types:

- **Ordinances (Switzerland (draft), Germany, EU):** even though the Swiss ordinance on automatic driving is still work in progress, some elements are already useful for the validation of very general operational requirements. The corresponding EU Commission Implementing Regulation and the German ordinance are already in force. Even though not valid in Switzerland, they are still useful as examples of how teleoperated driving is treated in the neighbouring countries and with a focus on harmonization of European regulations of ToD
- **UNECE regulations:** these provide functional and performance requirements for a number of vehicle parts which are also crucial in teleoperated vehicles, such as camera-monitor systems or the design of warning elements. Also, some regulations concerning current driver assistance systems can be applied to ToD with minor adaptations. The UNECE regulations are valid in Switzerland as well as in most other European countries. Often, they are based on or referring to an ISO standard
- **ISO standards:** similarly to UNECE regulations, some ISO standards already directly or indirectly cover several aspects of ToD. As the UNECE regulations are often based on or referring to ISO standards (more precisely speaking, they provide the legally binding implementation of the standards), there is an overlap between the fields of application to ToD
- **BSI standards (UK):** while the standards mainly target the UK, BSI provides a few innovative papers on definitions concerning ToD. However, for validation purposes, BSI standards only serve as comparative reference.
- **RFC standards:** published by the “Internet Society” NGO, these standards define the communication protocols used and respected internationally in the World Wide Web. While mostly not directly related to ToD, some definitions in the context of network latencies are useful for indirect validation of the proposed requirements

4.5.3.2 Scenario-based validation

Scenarios relevant to ToD have been identified within WP 2. They cover the problems which occurred in initial practical tests with ToD on public roads. The proposed requirements should provide solutions to all scenarios, so the known issues can be avoided. On the other hand, the scenarios also provide a possibility to check the completeness of the proposed set of requirements. The solution routes proposed within the scenario descriptions explicitly require a number of functionalities of the ToD systems. Consequently, a set of minimal requirements should include the corresponding functional requirements making sure that the proposed solution routes are in principle feasible. Therefore, the scenario-based validation method consists in checking that, for each functionality required by the list of scenarios, the proposed list of requirements contains a corresponding requirement. These requirements are mostly functional, but in some cases also operational or performance requirements.

While the scope of this method is limited to a qualitative validation mostly of functional requirements, it is the only validation method that allows a completeness check on the list of requirements. However, this check provides only a necessary, not a sufficient criterion.

4.5.3.3 Validation of performance values with theoretical and experimental methods or based on scientific literature

Performance requirements are particularly challenging to validate. To assess the performance of the system, a quantitative performance measure of some sort is needed. During validation, not only does an appropriate performance measure in alignment with the ToD context have to be selected, but the required performance threshold has to be both sufficient and realistic for a ToD system.

In some cases, particularly concerning aspects inherited from conventional vehicles, a validation based on existing standards is possible. Also, a scenario-based validation may be applicable sometimes; however, this method rather provides an additional check. When it comes to performance aspects inherent to teleoperated driving, a dedicated experimental or theoretical validation can be required to establish and check suitable performance thresholds. This can be achieved with different approaches:

- Estimation of the minimal performance value with a simplified theoretical model
- Laboratory or field tests with a teleoperated vehicle
- Literature research for suitable theoretical models or experimental data available in scientific publications

In case suitable results are available in the scientific literature, it must first be verified that the models or data are actually applicable to the requirement being validated. In some cases, modifications or additional experiments might be necessary.

In the context of ToD, a particularly critical performance measure is the network latency delaying the data transfer from the vehicle to the control centre and vice-versa. There are no prototypes for latency requirements in conventional road vehicles, so a validation of latency requirements cannot be based on existing standards. Therefore, the theoretical and experimental validation of that value will be presented in more detail than other methods in the following chapter.

4.5.4 Application and Results

4.5.4.1 Application of existing standards

For several requirements, the validation could be performed based on existing standards. Table 17 contains an overview of the standards, regulations, and other sources considered for the validation. Some of these sources were directly or indirectly applied to validate requirements (in that case, it is indicated in the respective columns). Others were either used for comparative purposes or considered not applicable. Even the sources that were considered not applicable within the current project were indicated in the list, as they might be useful for future modifications.

In some cases, the coverage of the different sources overlaps. This is because they are to some extent based on each other (e.g., the UNECE regulations often implement ISO standards). However, for the same reason, there are rarely contradictions between the sources. If that were the case, either the sources would have to be prioritized according to their relevance under Swiss law, or an additional validation, e.g. based on experiments or scientific studies, would be needed. Fortunately, no such case was encountered.

Existing regulations, standards and application for validation of requirements

Type	Title	Valid in	Applicable in CH	Applicable requirements
Ordinance (draft)	OCA	Switzerland	In preparation	RROLO10 RROLO60 RROLO90
Ordinance	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426	EU	No	RROLO70 RROL130 RROL160 RROL240 RSB160130 RSB140 RSB200-220
Regulation	UN Regulation No. 13 - regard to braking	UNECE member states	yes	-
Regulation	UN Regulation No. 46 - indirect vision	UNECE member states	yes	RSB270
Regulation	UN Regulation No. 79 - regard to steering equipment	UNECE member states	yes	-
Regulation	UN Regulation No. 121 - location and identification of hand controls, tell-tales and indicators	UNECE member states	yes	RSB260 RSB280 RSB290
Regulation	UN Regulation No. 125 -	UNECE member states	yes	-

Type	Title	Valid in	Applicable in CH	Applicable requirements
	forward field of vision			
Regulation	UN Regulation No. 151 - Blind Spot Information System for the Detection of Bicycles	UNECE member states	yes	-
Regulation	UN Regulation No. 155 - cyber security	UNECE member states	yes	CR0010 – CR0090 CR1010-CR0120 CR120 CR1590 CR1610 CR1750 CR1760
Regulation	UN Regulation No. 156 - software update	UNECE member states	yes	CR1600 CR1680 CR1690
Regulation	UN Regulation No. 159 - Moving Off Information System for the Detection of Pedestrians and Cyclists	UNECE member states	yes	-
Regulation	UN Regulation No. 160 - event data recorder (EDR)	UNECE member states	yes	-
Ordinance	008-verordnung-automatisierte-autonome-fahrfunktion	Germany	no	-
Standard	ISO 11992-1 Road vehicles – Interchange of digital information on electrical connections	international	yes	
Standard	ISO 16505:2019 - performance aspects of Camera	international	yes	RSB0320 RSB0330 RSB0340 RP010-RP160
Standard	ISO 2575; 2021 – symbols for controls, indicators and tell-tales	international	yes	RSB310 RSB350

Type	Title	Valid in	Applicable in CH	Applicable requirements
Standard	ISO 7010; 2019 - Graphical symbols - Safety col- ours and safety signs- Registered safety sign	international	yes	RSB220
Standard	BSI FLEX 1886	UK	no	-
Standard	BSI FLEX 1890	UK	no	-
Standard	RD_Advice- paper_LC	UK	no	-
Standard	RFC 1242	international	yes	-
Standard	RFC 2679	international	yes	-
Standard	RFC 2681	international	yes	-

Table 17: Existing regulations, standards and applications for validation of requirements

4.5.4.2 Scenario-based validation

The relevant scenarios as identified in WP 2 could be applied to validate a number of requirements. Some requirements are covered by several scenarios. Each scenario contains one or several solution options using different ROLs. Therefore, some of the requirements apply differently according to the respective ROL; this is also a result of the use of scenarios.

Use of scenarios for validation

Scenario name	ROLs used	Applicable to requirements
Scenario 1: Unexpected road blockage	4, 3, 2	RSB020
		RSB030
		RSB040
		RSB050
		RSB080
		RSB090
		RSB110
		RSB120
		RSB130
		RSB140
		RSB150
		RSB170
		RSB190
		RSB200
		RSB230
		RSB240
RSB250		

Scenario name	ROs used	Applicable to requirements
Scenario 2: Loss of network connectivity or poor network performance	4, 1	RSB020 RSB050 RSB240
Scenario 3: Imprecise location due to location system issue or signal loss	2, 1	RSB020 RSB030 RSB070 RSB130 RSB170 RSB190 RSB200 RSB240
Scenario 4: Malfunction of optical sensor systems due to solar radiation	2, 1	RSB020 RSB030 RSB130 RSB160 RSB170 RSB190 RSB200 RSB240 RSB300
Scenario 5: GNSS and odometer give ambiguous results due to slippery road	4, 3, 2, 1	RSB020 RSB030 RSB050 RSB070 RSB080 RSB090 RSB130 RSB170 RSB190 RSB200 RSB240
Scenario 6: Adverse weather conditions	3, 2, 1	RSB020 RSB030 RSB050 RSB080 RSB090 RSB130 RSB150 RSB170 RSB190 RSB200 RSB230 RSB240 RSB270

Scenario name	ROIs used	Applicable to requirements
Scenario 7: Bottleneck in dense traffic	4, 3, 1	RSB020
		RSB030
		RSB040
		RSB050
		RSB080
		RSB090
		RSB130
		RSB150
		RSB170
		RSB180
		RSB190
		RSB200
		RSB210
		RSB230
		RSB240
RSB250		
RSB270		
Scenario 8: False positive obstacle detection	4, 3, 2, 1	RSB020
		RSB030
		RSB040
		RSB050
		RSB080
		RSB090
		RSB130
		RSB150
		RSB160
		RSB170
		RSB180
		RSB190
		RSB200
		RSB210
		RSB230
RSB250		

Table 18: Use of scenarios for validation

4.5.5 Validation of Performance Values with Theoretical and Experimental Methods for the Latency Requirements

4.5.5.1 Definitions

In the mobile networks used for ToD, network latencies appear in different processes; therefore, several different latency definitions apply. In the context of ToD, the following latency measures are useful (Figure 63):

- **Uplink video latency (glass to glass):** latency from on-board video capture to screen in Remote Control Centre (including video encoding and rendering)
- **Uplink data latency:** travel time of data from vehicle to remote operation centre
- **Downlink data latency:** travel time of data remote operation centre to vehicle
- **Roundtrip latency:** sum of uplink video and downlink data latency
- **Service level latency:** total latency from event occurrence to activation of actuators, including video encoding and rendering and reaction time of human user

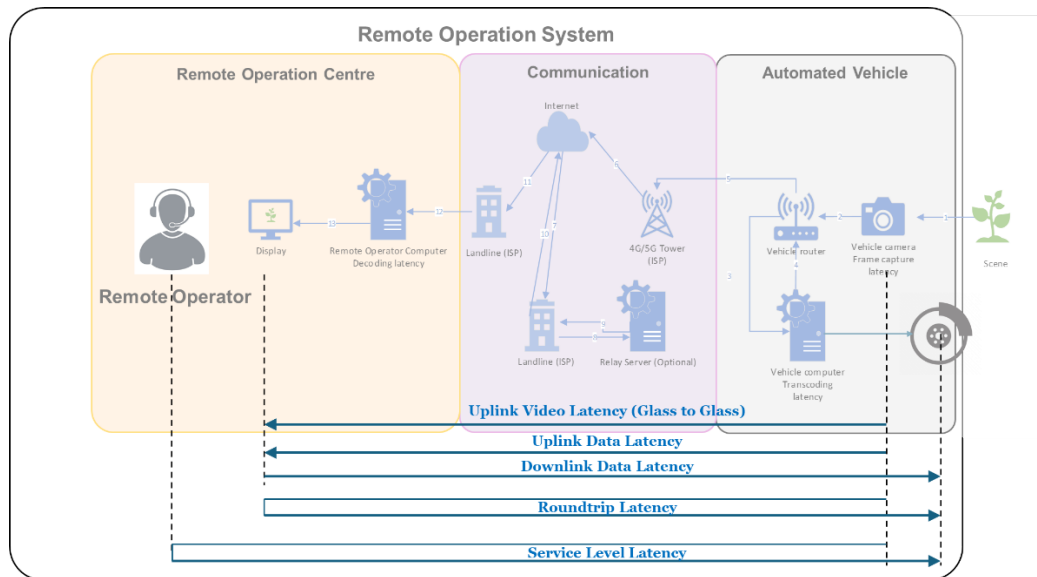


Figure 63: Definition of latencies

Performance requirements concerning network latency

ID	Category	ROL	Requirement Description	Source
RROLO80	Communication	ROL2	During ROL2, the roundtrip latency (from AV camera to remote operation centre and from remote operation centre to AV actuators) shall be less than 850 ms.	Own experience
RROL200	Communication	ROL3	During ROL3, the roundtrip latency (from AV camera to remote operation centre and from remote operation centre to AV actuators) shall be less than 700 ms.	[72] [73]

Table 19: Network latency performance requirements

4.5.5.2 Latency requirements

Network latencies are addressed by the requirements summarized in Table 19. The required latencies are different depending on the current ROL, see Table 20. In ROLs 4 and 5, there are no requirements on the acceptable latency. The requirements for ROL 3 are stricter than for ROL 2. This is due to the higher speeds which are permitted at ROL 3. A short summary of the required maximum latencies is given in Table 20. The requirements for ROL 3 are based on existing literature [72] and [73]. For the low speeds permitted at ROL 2, no literature values were available, so an own estimate had to be found. It was confirmed by the driving tests carried out in the experimental part of the present project that the proposed values are sufficient to ensure a safe operation at ROL 2.

Summary of maximum latency requirements according to ROL

ROL	Maximum Roundtrip latency (ms)
ROL5	Not specified
ROL4	Not specified
ROL3	700
ROL2	850

Table 20: Summary of maximum latency requirements according to ROL

4.5.5.3 Effect of latency on braking distances

As a first approach to assess the effect of roundtrip latency on the safe operation of the vehicle, the increase in braking distance can be computed and compared to acceptable braking distances of a conventional vehicle.

Based on the assumption of a braking deceleration which grows linearly during build-up time t_b to a constant value a , the braking distance ΔS_c needed by a conventional vehicle for a full stop from an initial speed v can be computed as

$$\Delta S_c(v, t_r) = v (t_r + t_b) + \frac{1}{6} a t_b^2 + \frac{1}{2a} \left(v - \frac{1}{2} a t_b \right)^2 \quad (1)$$

where t_r is the reaction time of the driver. With the gravitational acceleration g and the coefficient of friction μ of tyres on the road, the peak acceleration is $a = \mu g$.

In a remotely driven vehicle (ROL2), the roundtrip latency t_l effectively adds to the reaction time of the (remote) driver, as it increases the time between the occurrence of the event triggering the braking manoeuvre and the activation of the brakes. Therefore, the braking distance of a teleoperated vehicle reads

$$\Delta S_t(v, t_l, t_r) = \Delta S_c(v, t_r) + v t_l \quad (2)$$

Assuming typical values of $\mu = 0.7$, $t_b = 0.2s$, a constant latency $t_l = 0.2s$ and a Remote Operator reaction time $t_r = 0.8s$, the braking distances at different initial speeds are as displayed in Figure 64. The differences are in the order of magnitude of 10 – 30%, with values up to 4m.

A conventional vehicle rolling at the speed limit \hat{v} valid in the current traffic situation has the braking distance

$$\Delta\hat{S} = \Delta S(\hat{v}, t_r) \quad (3)$$

With a typical human reaction time of 0.8 – 1s, this is the braking distance considered acceptable for a conventional vehicle in a standard traffic situation. A teleoperated vehicle in the same traffic situation must not exceed this braking distance. Even though, in most situations, an emergency braking manoeuvre of a teleoperated vehicle will likely be triggered by an automated emergency braking (AEB) system (reacting considerably faster than a human driver and thus coming to a stop within a distance much shorter than $\Delta\hat{S}$), in the worst-case scenario of the remote operator reacting to an event which the AEB system has missed, it has to be ensured that the braking distance ΔS_t does not exceed this value.

In order to respect the acceptable braking distance, the speed of the teleoperated vehicle can be limited to a value $v_t < \hat{v}$. At a given latency t_l , the highest speed \hat{v}_t at which the condition $\Delta S_t(v_t, t_l, t_r) \leq \Delta S(\hat{v}, t_r)$ is satisfied can be computed to

$$\hat{v}_t = -a \left(t_r + \frac{t_b}{2} + t_l \right) + \sqrt{\hat{v}^2 + 2a\hat{v} \left(t_r + \frac{1}{2}t_b \right) + a^2(t_r + t_l + 0.5 * t_b)^2} \quad (4)$$

The maximum possible speeds according to this expression are displayed in Figure 65. At a latency of 0.3s, a speed reduction of approximately 10-20% is required. This approach might be of interest for applications where a teleoperated vehicle is driving close to the speed limit which, however, for the probable application cases of ToD in the close future will likely not be the case.

In some of the use cases of ToD discussed currently, the teleoperated vehicle will likely – at least at ROL 2, i.e. manual remote driving – be limited to a speed well below the speed limit valid for conventional vehicles on the same street, such as 6 km/h in zones with speed limits of 20 -50 km/h. In these cases, it makes more sense to compute the highest acceptable latency at the given speed v_t of the teleoperated vehicle which respects the acceptable braking distance according to the speed limit. This latency is given by

$$\hat{t}_l = \frac{\hat{v} - v_t}{v_t} \left(t_r + \frac{1}{2}t_b \right) + \frac{\hat{v}^2 - v_t^2}{2av_t} \quad (5)$$

As show in Figure 66, the acceptable latencies according to this equation at speeds < 10 km/h (while the speed limit would allow 20 – 50 km/h) are in the order of magnitude of one to even several seconds, which is well above the values which typical ToD systems are able to achieve in current mobile networks.

In conclusion, roundtrip latencies potentially have a considerable influence on braking distances of remotely driven teleoperated vehicles as compared to conventional vehicles, increasing the braking distance by several meters at typical urban speeds. Even though this effect only plays a safety critical role in the rare event of an AEB system failure, it will require vehicles in remote driving mode to travel at speeds below the current speed limit, provided that the braking distance of a conventional vehicle is considered the acceptable limit. If the speed of the teleoperated vehicle is limited to a value close to the general speed limit in (parts of) the ODD, the approach presented above provides a useful way to compute upper limits on acceptable latency values. Performance requirements on acceptable network latencies can either be inferred or validated with this approach.

When applying the results to the latency requirements proposed in the current framework, it turns out that the proposed round-trip latency requirements of 700 ms in ROL2 are, at the low speeds allowed at this ROL (6 km/h max.), very well within the acceptable limits (at a speed limit of 30 km/h, a latency of 5700 ms would be allowed). The braking distance at 0.8s reaction time at this speed is 2.86m (compared to 12.5m of a conventional vehicle rolling at 30 km/h). However, for such a vehicle in remote driving mode, the limiting factor for acceptable network latencies could be something other than braking distance, such as the general manoeuvrability of the vehicle and the precision of steering. A performance requirement on network latency should make sure that generic vehicle manoeuvres such as lane keeping, cornering or parallel parking can be executed sufficiently precisely. This highlights the need for additional physical validation tests of latency requirements.

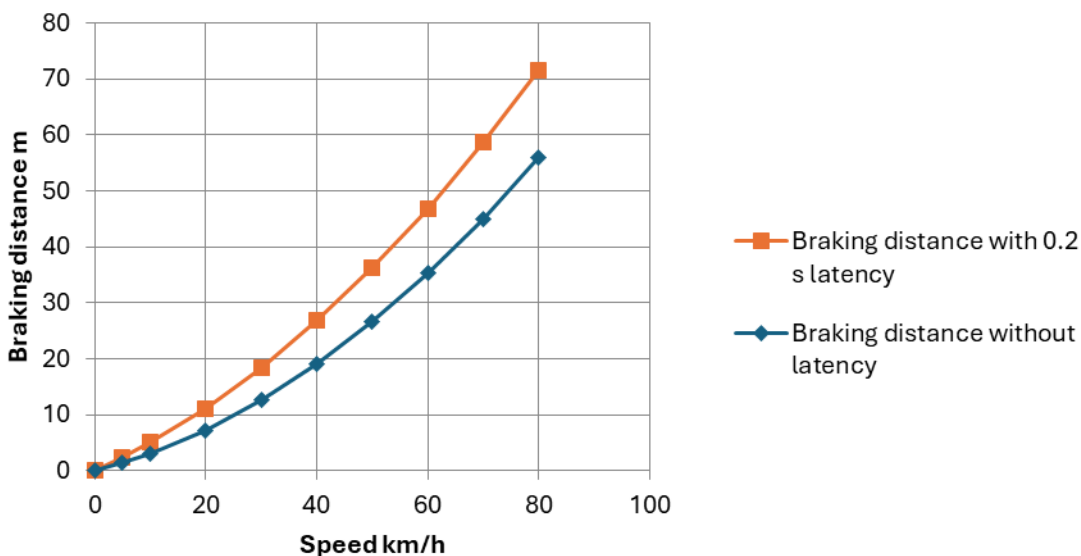


Figure 64: Braking distance vs. speed with and without latency

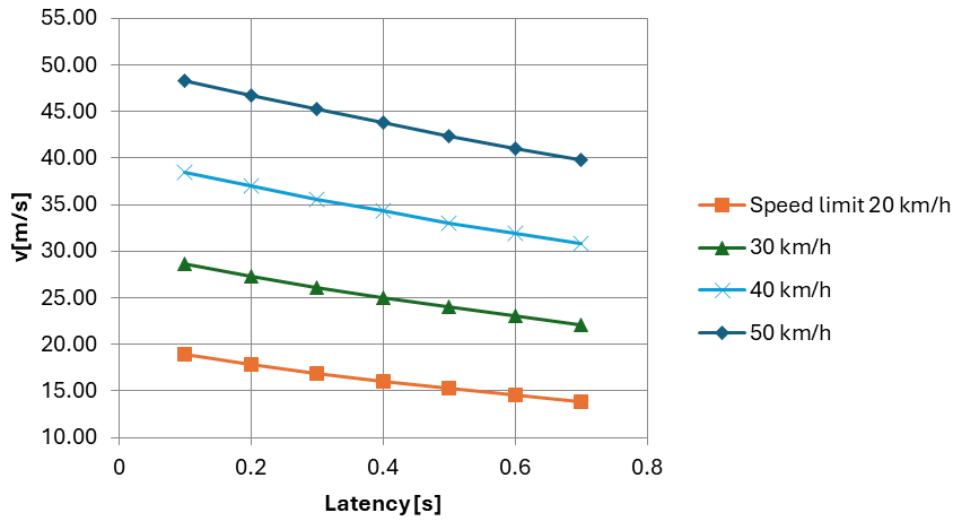


Figure 65: Highest possible speed \hat{v}_t of the teleoperated vehicle to maintain braking distance of conventional vehicles (0.8s reaction time)

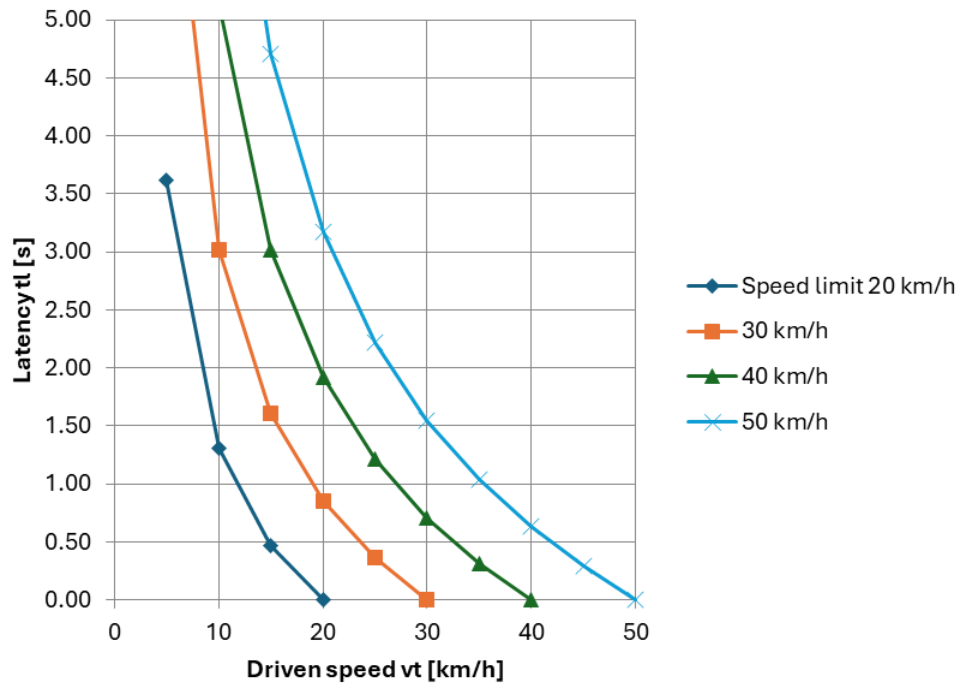


Figure 66: Highest acceptable latency \hat{t}_t of the teleoperated vehicle as function of the speed (0.8 s reaction time)

4.5.6 Cybersecurity

Cybersecurity requirements can be validated in multiple ways. Process requirements can be validated through an organizational audit against specific norms or regulations. Technical requirements can be validated at different levels (from unit tests to integration testing) to assess the integration of components within the system. At a higher level, fuzzing or pentesting can be performed:

- **Fuzzing** involves inputting large amounts of random data, or “fuzz”, into the system to identify potential vulnerabilities and unexpected behaviours. This method can uncover security flaws that might not be detected through conventional testing methods
- **Penetration testing**, also known as pentesting, is a method where security experts simulate cyber-attacks on the system to identify and exploit vulnerabilities. This helps in understanding how an attacker could gain unauthorized access and what potential damage could be done. Penetration testing provides a practical assessment of the system’s security posture and helps in identifying areas that need improvement

Fuzzing and penetration testing can also be considered validation activities, not just verification activities. Validation activities aim to ensure the right product is built; in the context of cybersecurity, this means ensuring the product is secure enough. In contrast, verification activities ensure the product is built correctly, meaning all requirements have been correctly implemented. This is why penetration testing can be considered both a verification activity, ensuring that requirements are correctly implemented, and a validation activity, ensuring that no requirements have been forgotten.

The differentiation between verification and validation is very important in the context of cybersecurity requirements. Cybersecurity is a rapidly evolving field, with new threats and vulnerabilities emerging daily from diverse attack vectors, including local attacks (direct connection to an ECU or vehicle part) and network attacks (through the communication interface between the AV and its backend or Remote Operation Centre). Requirements for Remote Operation Centre that pass verification today may no longer meet cybersecurity standards in the coming months or years. Therefore, continuous system monitoring and regular testing are critical to ensure that the Remote Operation System reflects the state-of-the-art in cybersecurity. Consequently, validation activities will go beyond only testing the requirements stated in this document.

Due to resource constraints, the cybersecurity part of the project focused more on the requirement elaboration than the validation part. Only pentest activities have been performed in this project to verify some of the cybersecurity requirements. The methodology and results are described in section 4.7.

4.5.7 Summary

In this chapter, the validation methods used within this project and their results are presented. Validation, in this context, is defined as a check that (i) the proposed requirement addresses a relevant problem, (ii) the proposed numerical values of physical quantities are sufficient and can realistically be achieved, and (iii) the requirement is in accordance with existing regulations or norms if applicable.

The proposed validation method consists of three main strategies, namely the application of existing standards and regulations, validation by scenarios, and validation of performance values with theoretical and experimental methods. The first strategy is in most cases the preferred one, as it directly verifies point (iii). A scenario-based validation is in many cases useful in addition to the other strategies, as it can, on top of verifying point (ii), be used as a check of the set of requirements for completeness. Theoretical or experimental validation is crucial for critical performance values, and additional experimental efforts can sometimes be avoided by using existing results from the scientific literature.

The application of this validation methodology to the proposed set of requirements showed that, in spite of dealing with a new mode of transportation, validation by existing standards and regulations could be applied widely; in some cases, standards designed for slightly different applications could be used with slight modifications. While scenario-based validation was only used as an additional check, theoretical or experimental validation was applied to the most critical performance parameters for ToD, which are network latencies. The proposed latency requirements, which were derived from the scientific literature, were checked with a driving-dynamics based theoretical approach for their effect on braking distances, showing that the proposed values are far from being critical in this respect.

4.6 Testing on Site

On-site testing is a critical component of this research, providing practical insights into the performance and reliability of existing remote operation systems from LOXO and BFH under real-world conditions. This section describes the testing procedures conducted in controlled environments that simulate actual road scenarios. These tests are designed to evaluate the effectiveness of the system in meeting the defined requirements, as well as to identify any potential challenges or limitations. The results from these on-site tests offer valuable data, helping to refine the system and ensuring it is prepared for deployment in public settings.

These tests were part of, or rather an extension to, the validation methodology described in chapter 4.5 to test the soundness and completeness of the proposed requirements for teleoperated driving. As mentioned in section 4.5, network latencies are a crucial aspect of teleoperated driving and the performance requirements addressing latencies are particularly difficult to validate in view of the almost complete lack of existing regulations in this specific area. Hence, the first focus of the present test series was on the validation of network latency requirements or, more precisely speaking, the effect of network latencies on the manoeuvrability of teleoperated vehicles at low speeds.

Another area of focus was an exemplary demonstration of a scenario-based validation, where the “false positive obstacle detection” scenario (referred to as “false positive scenario” in the section 4.1) was chosen to demonstrate that, with the two available test AVs, a solution is feasible with the ROLs proposed in the requirements framework.

Therefore, the following **research questions** were defined for the test series to address:

- Up to which latency is reliable manoeuvring of a teleoperated vehicles at ROL2 (Tele Driving) possible? Are the limit values defined in the proposed requirements within this range?
- Can the false positive scenario reliably be solved with the test vehicles and the defined ROLs?

A detailed discussion of the literature on the topic is offered in section 4.4; only the most relevant sources shall be mentioned here. Neumeier [72] performed driving simulator tests with different latencies at speeds ranging from 15 – 38 km/h and observed significant impacts on driving performance at one-way latencies beyond 300 ms. Davis et al. [74] concluded from volunteer experiments in driving simulators that round-trip latencies of about 700 ms should not be exceeded. However, these tests were carried out at considerably higher speeds than the tests presented in this work.

4.6.1 On-Site Test Concept and Instrumentation

4.6.1.1 On-site test concept

In order to address the research questions formulated above, three types of tests were planned, which were each to be performed with the two teleoperated vehicles available to the project (LOXO and BFH Smartshuttle):

1. **Slalom tests**
2. **Parking tests**
3. **Tests Scenario 8 - False positive obstacle detection**

The tests were chosen in a way to cover different driving manoeuvres at increasing latencies as well as the chosen sample scenario. All tests were set up on the test-driving range of the project partner DTC, with its local 4G/5G-network (70% of bandwidth reserved for testing and research). The vehicles were teleoperated via the 4G mobile network from Remote Operation Centres (Figure 67) which were located either on the DTC area (BFH Smartshuttle) or in Fribourg (LOXO).

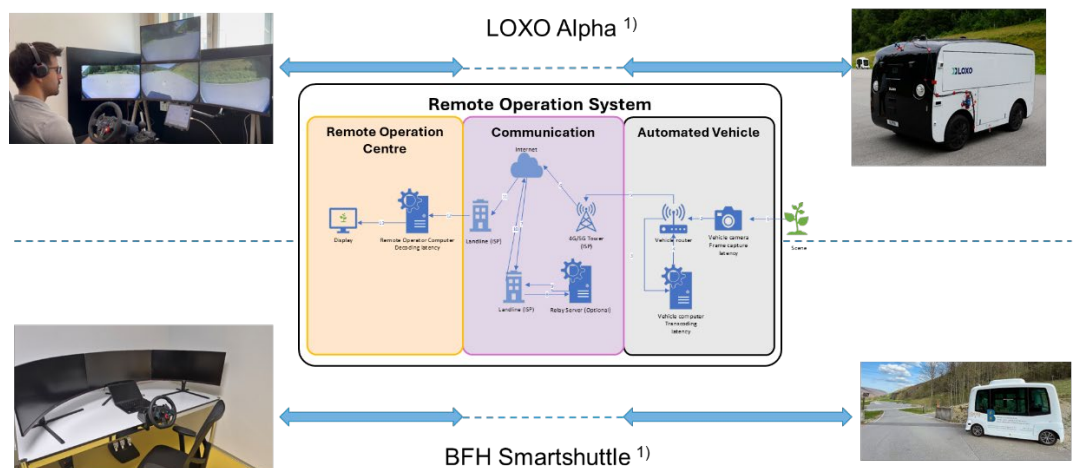


Figure 67: Test set-up LOXO Alpha and BFH Smartshuttle with Remote Operation Centre using the communication network at DTC

The inherent video latency (glass to glass) of this network configuration was in both cases around 110 ms. By simulating additional latency in the control computer of the AVs, the video latency as experienced by the Remote Operator could be adapted to any value greater than the inherent latency. The latency was monitored continuously in each Remote Operation centre.



Figure 68: Aerial view, DTC test drive area, slalom and parking testing tracks

1. Slalom tests at different latencies

In this test, the teleoperated vehicle, while operating at ROL2, followed a slalom consisting of three consecutive half circles of 8m radius (Figure 68). Prior to the tests, a slalom course with 8 m centre line radius and 3 m lane width was marked with red tape on the test-driving range (Figure 69). For each test round, the vehicle waited for a short moment in the start position (cones on the left Figure 69), then the teleoperator navigated it manually through the course, trying to follow its centre line. The speed was limited to 6 km/h (according to the guidelines for ROL2). In the end position (cones on the right), the vehicle stopped again for a few seconds prior to returning to the start position. This test round was done at least three times per tested latency level. With each vehicle, the following latency levels (glass to glass latency) were tested: 110 ms (baseline), 250 ms, 400 ms, 550 ms, 700 ms, 850 ms, 1250 ms. Prior to the test runs, each teleoperator had time to do a few training-runs to get acquainted with the course.

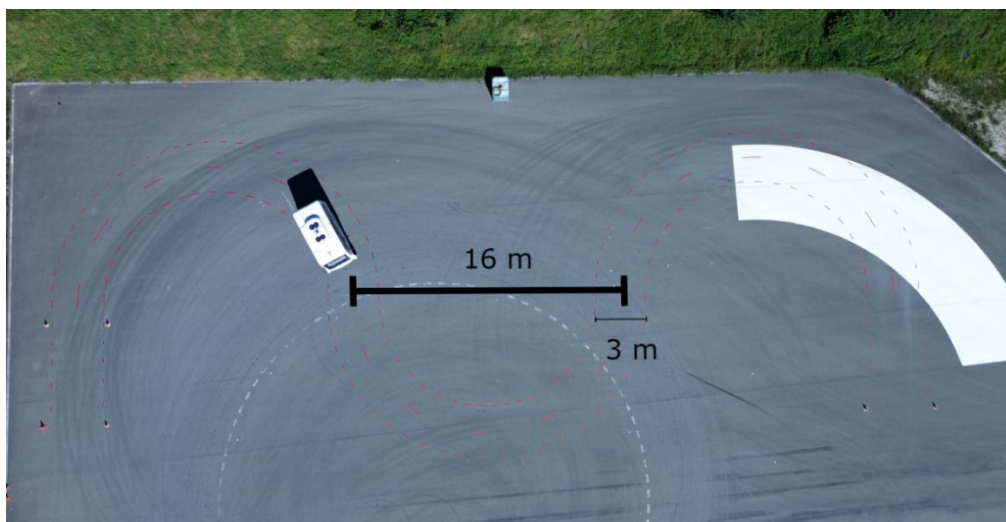


Figure 69: Aerial view of the slalom course

2. Parking tests

This test emulated a parallel parking manoeuvre. A parking spot of dimensions 6 m by 4 m was marked with cones at 1 m distance from a marked two-lane road of 25 m length (Figure 70). After waiting for a short while in the start position at the beginning of the lane, the Teleoperator navigated the vehicle at ROL2 to the parking spot and did a forward parallel parking manoeuvre (both vehicles have two-axle steering). After the parking position was reached, the Teleoperator rolled the vehicle in forward direction back onto the driving lane to the final position at the end of the lane (Figure 71).

The test was carried out at latencies of 110 ms (baseline), 550 ms, 850 ms and 1000 ms, repeating each test several times. Prior to the tests, each teleoperator could do a few training runs.

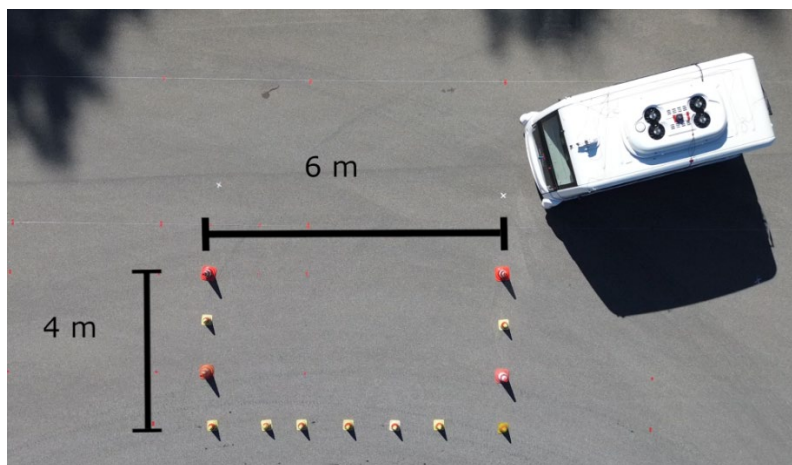


Figure 70: Setup for the parking tests

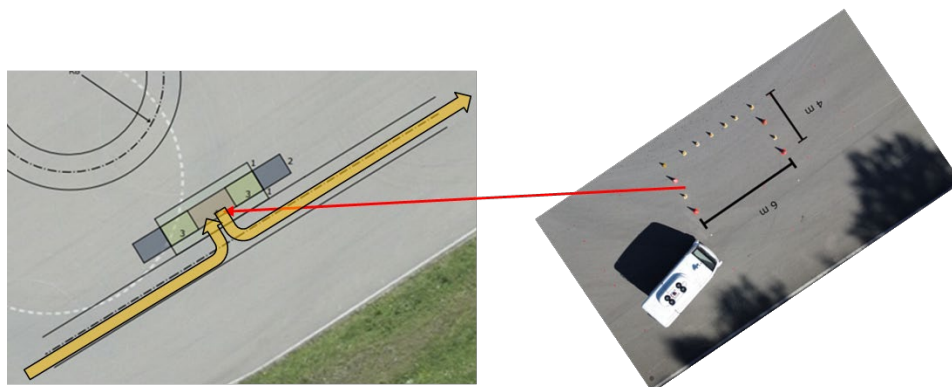


Figure 71: Parking test procedure

3. Tests of the false positive scenario

The false positive scenario was tested on the marked two-lane road of 25 m length also used for the parking tests. At a point about half-way along the road, an obstacle was placed in the right lane (Figure 72). Two different kinds of obstacles were used: either a bundle of leafy branches held in place by a plastic cup, or an empty paper bag. A human driver would likely not consider either of them as relevant obstacles – hence, they will be referred to as non-obstacles in the following. Nevertheless, they are big enough for an AEB system to trigger an emergency stop.

From the start position, the vehicle followed the lane at ROL2 (BFH Smartshuttle and some tests LOXO) or at ROL5 (some tests LOXO) until the AEB system triggered an emergency stop after detecting the obstacle. Afterwards, the teleoperator tried to solve the scenario using ROL2. Two solutions were tested: bypassing on the left lane and running over the obstacle at very low speed, where the AEB system is inactive. The tests were repeated several times. All tests were performed at the inherent network latency of 110 ms.



Figure 72: Setup for scenario test with "false positive"-obstacle in place

4.6.1.2 Teleoperated vehicles

Two teleoperated vehicles (LOXO and BFH Smartshuttle) were available to the project. All tests were carried out with both vehicles, for which a short technical description is provided below.

1. LOXO Alpha

LOXO operates its own fleet of delivery vehicles, featuring the seamlessly integrated LOXO Alpha and the LOXO Buzz, a retrofitted delivery van. For the tests carried out at the DTC, the LOXO Alpha (Figure 73) automated vehicle was used. LOXO Alpha is specifically designed for efficient last-mile delivery.



Figure 73: LOXO Alpha automated vehicle for last mile delivery

Technical data LOXO Alpha

Item	Details
Manufacturer	LOXO
Identifier	LOXO Alpha
Type of vehicle	L7e-CU (without passenger on board)
Fuel code	Electric
Length [m]	3.5
Width [m]	1.5
Height [m]	1.9
Max speed [km/h]	30
Tare weight [kg]	800kg
Total weight [kg]	1200kg
Body shape	Elongated rectangle
Transmission	Direct, 1 electrical motor per wheel
Seats	0
Engine	Electric 72VDC
Emissions	0g/km
Energy label	A

Table 21: LOXO Alpha technical data

The LOXO Alpha vehicle was piloted from a Remote Operation Centre (Figure 74) located at LOXO's offices in Fribourg and includes the following components:

- 4 x 27" screens
- 1 computer
- 1 pedal and steering wheel
- 1 seat
- 1 tablet for telemetry (vehicle status information)



Figure 74: LOXO Remote Operation Centre in Fribourg

2. BFH Smartshuttle

The Bern University of Applied Sciences and its Institute for Energy and Mobility Research manages their own automated vehicle projects featuring the seamlessly integrated BFH automated system across multiple vehicles, such as the BFH Smartshuttle (Figure 75). The BFH Smartshuttle is an advanced automated shuttle specifically designed for urban transportation.



Figure 75: BFH Smartshuttle automated vehicle for people transportation

Technical data BFH Smartshuttle

Item	Details
Tire size	195/65R16C
Tire pressure	4.2 bar
Track width	1381 mm
Wheelbase	2800 mm
Length	4050 mm
Width	1970 mm (1892 mm)
Height	2871 mm (with A/C)
Curb weight	2130 kg
Total weight	3030 kg
Payload	900 kg
Drive	2 electric motors, each 8 kW
Operating voltage	Drive: 48 V, other systems: 12 V
Maximum speed	13 km/h (software-limited)
Battery life	10 – 15 hours
Brakes	Regenerative braking, 4 hydraulic disc brakes, electric parking brake, fail-safe axle brake
Steering	Electric, symmetric on both axles
Turning circle	8 m (turning radius)
Level of automation	L4 (High automation, low-speed shuttle)

Table 22: BFH Smartshuttle technical data

The Remote Operation Centre (Figure 76) is in the offices of the Technical Vehicle Laboratory of the Bern University of Applied Sciences located in Vauffelin. It includes the following components:

- 3x 32" curved screens
- 1x steering wheel and pedal controller
- 1x laptop
- Seat



Figure 76: BFH Remote Operation Centre in Vauffelin

4.6.1.3 Measurements and instrumentation

Prior to the tests, the test vehicle was instrumented with the following equipment:

- RaceLogic VBox 3i-ADAS-V1 data logger (100 Hz GNSS data logger)
- VBox Inertial Measurement Unit (IMU)
- Racelogic NTRIPMDM-V1 modem (GNSS position correction via NTRIP)
- Racelogic VBox Video HD2 (two cameras on the outside of the vehicle)

Photographs of an equipped vehicle are shown in Figure 77 and Figure 78.



Figure 77: Measurement equipment on LOXO Alpha



Figure 78: Antenna and camera positioning on LOXO Alpha

On-board sensors recorded the following quantities:

- position of the GNSS receiver with 2cm accuracy
- triaxial accelerations
- triaxial angular velocities
- temperature
- synchronised on-board video recordings (front and side view)

The sampling rate of GNSS and Inertial Measurement Unit (IMU) was 100 Hz. Furthermore, the tests were recorded by one stationary video camera. Some additional tests were also recorded by drone video. The total (inherent and artificially induced) network latencies were measured in the Remote Operation centre as a mean value prior to each test.

4.6.1.4 Network

The following diagram illustrates the network setup between the AV and the Remote Operation Centre used for the tests conducted at the DTC.

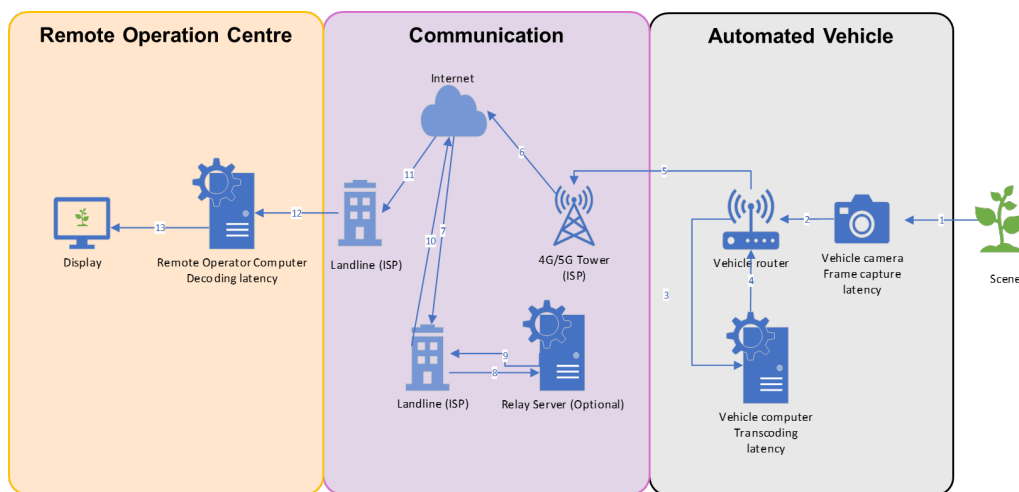


Figure 79: Network used for the tests on site at DTC

4.6.1.5 Analysis of location data

The Differential GNSS (DGNSS) system provided the precise location of the vehicle with a time resolution of 0.01s. The raw data was converted to metric easting and northing coordinates with origin at a defined point on the entrance of the test-driving range. The individual test runs were identified and split so that each run started from a comparable position.

For the slalom tests, the individual runs were parameterized by arc length and interpolated to ensure that all runs done with the same vehicle had the same sampling rate on the arc length parameter. Furthermore, a mean trajectory (arithmetic mean of E and N coordinate at each point of the trajectory) over all runs done with the same vehicle was computed. To compare each individual run to the mean trajectory, the area between the two trajectories was computed and divided by the total arc length. The resulting mean distance from the mean trajectory d_m of the individual run from the mean trajectory is a measure to how far during this individual run the teleoperator diverged from the mean trajectory (and, thus, from the best estimate of the intended course).

The mean distance from the mean trajectories was evaluated for all runs and averaged over runs under the same conditions (same vehicle and same latency) to investigate the effect of the latency on the precision of manoeuvring. No comparison was done

between runs driven with different vehicles, as the position of the GNSS sensor cannot be compared.

For the parking tests, the location data was only converted to metric and split into individual runs, as the mean distance analysis would not make sense on the somewhat arbitrary trajectories resulting from minor differences how the parking manoeuvre was initiated. The location data of the scenario tests was not analysed any further.

4.6.2 On-Site Test Results

4.6.2.1 Slalom tests

A total of 16 tests at latencies up to 1250 ms with at least three rounds each were performed. The tests were conducted at a maximum speed of 6 km/h, as required for teleoperated operations under ROL2. The Remote Operators described the Remote Driving at high latencies as challenging but feasible after some training.

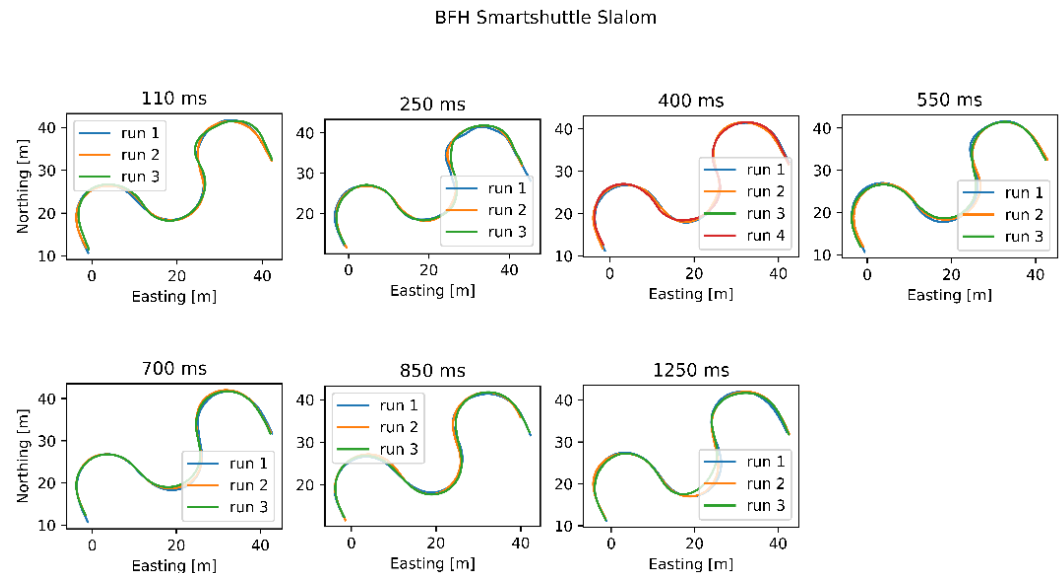


Figure 80: Location data of the BFH Smartshuttle slalom tests

The trajectories of the test done with the two vehicles are displayed in Figure 80 and Figure 81. In some of the trajectories of the LOXO tests, there are unrealistic spikes and jumps in the coordinates due to signal loss in the external DGNSS system used for logging, and not the vehicle's internal system. Consequently, the location data recorded during these tests cannot be considered reliable. Therefore, the tests at 110 ms (second test), 400 ms and 1250 ms latency were excluded from further analysis.

A plot of the mean distance from mean d_m for the BFH Smartshuttle and LOXO tests as a function of latency (Figure 82) shows that at latencies below 1000 ms, d_m remains below 0.4 m and approximately constant, with some variations due to the inaccuracy of manual driving (e.g., at 250 ms for BFH Smartshuttle). That is, the Teleoperator manages to follow the defined trajectory at about the same accuracy at these latencies. There is only one test at higher latencies with sufficient data quality, consisting of three runs with BFH Smartshuttle at a latency of 1250 ms (last data point in Figure 82). This test shows less precise steering, with mean distance from mean $d_m = 0.60$ m. However,

a one-sample test shows that this higher distance from mean is (just about) not statistically significant ($p = 0.058$).

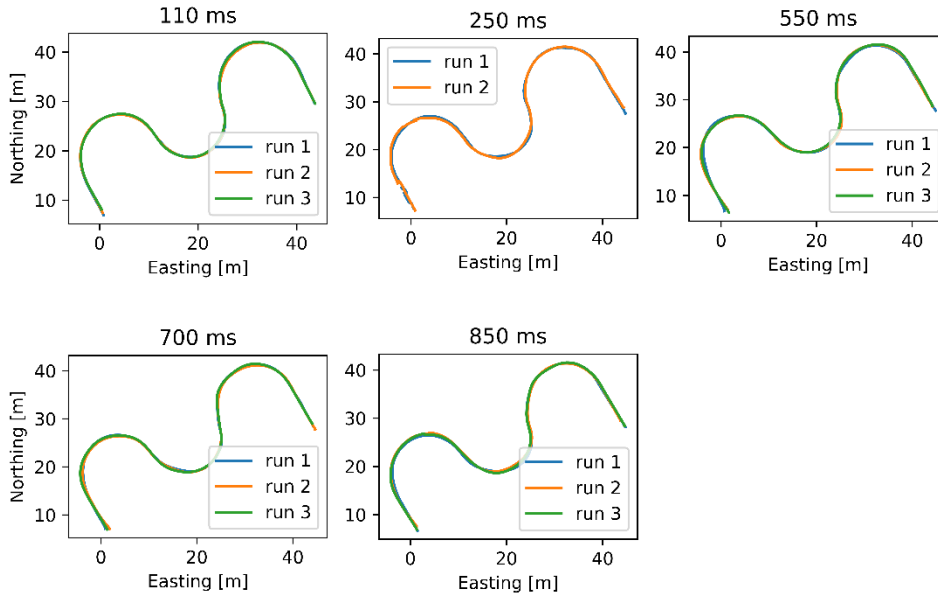


Figure 81: Location data of the LOXO slalom tests. Only test runs with sufficient data quality are shown.

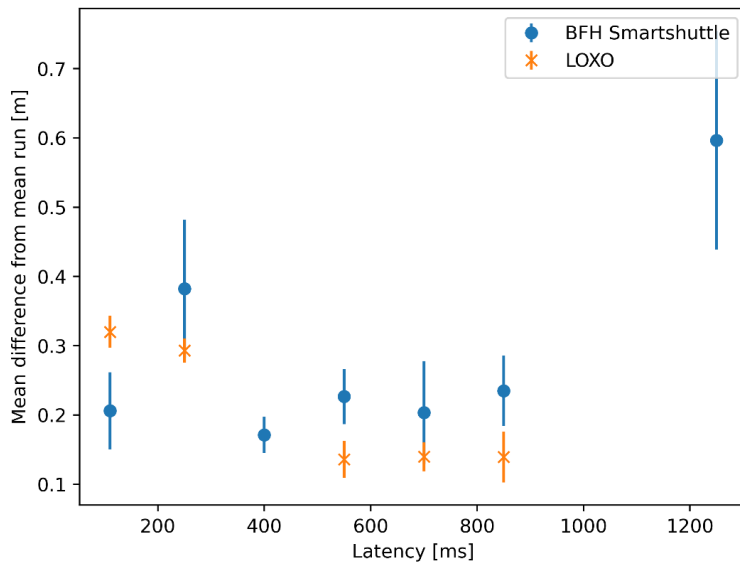


Figure 82: Mean distance from mean run for both vehicles. The error bars represent the standard deviation over all runs with the same latency

4.6.2.2 Parking tests

In total, 33 parking test runs were performed with the two vehicles. The two Remote Operators (Remote Operator A for BFH Smartshuttle and Remote Operator B for LOXO) reported not perceiving any noticeable influence of latency on their driving, likely due to the very low speeds used in these tests. However, parking manoeuvres were still considered somewhat difficult even at low latencies. It is worth noting that in the results, the "knocked cone" failures consistently occurred during the third attempt of the parking sequence. However, this is more likely due to coincidence or a lapse in concentration rather than a systematic issue. The trajectory plots of all tests are shown in Figure 80 and Figure 81.

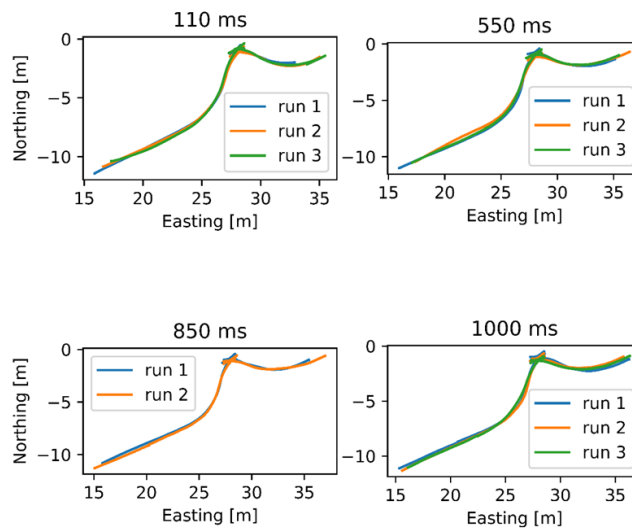


Figure 83: Parking tests BFH Smartshuttle

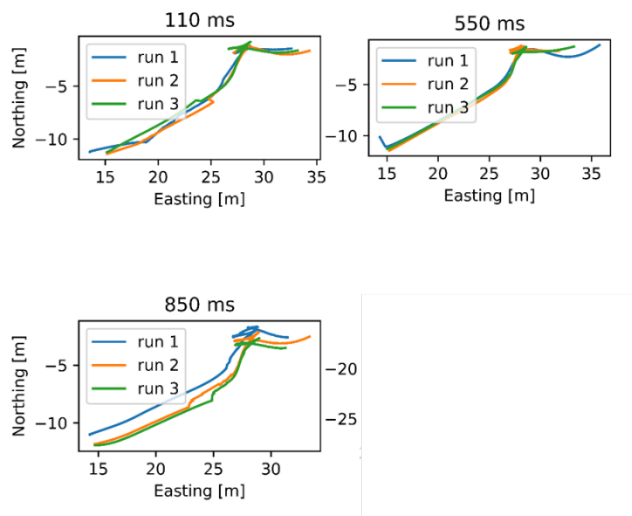


Figure 84: Parking tests LOXO Alpha

The evaluation of the parking tests was largely qualitative. Although the exact vehicle positioning data was collected for each test, success was determined based on whether

the vehicle stayed within the designated boundaries of the road and parking spot, and whether it avoided knocking down cones. The parking test results are shown in Figure 83 for the BFH Smartshuttle and Figure 84 for the LOXO Alpha (for which only test runs with sufficient data quality are included). Table 23 and Table 24 contain summaries of the results for the BFH Smartshuttle and LOXO Alpha vehicles across all the tests. All BFH Smartshuttle tests were carried out with Remote Operator A and all LOXO tests were carried out with Remote Operator B.

Criteria for success:

- The vehicle stays within the designated boundaries of the road and parking spot
- The approach, parking, and exit manoeuvres are performed with acceptable precision
- The vehicle does not hit or knock down any cones

Summary of parking tests BFH Smartshuttle

Vehicle	Pass.	Attempt	Latency (ms)	Approach	Parking	Exit
BFH Smartshuttle	1	1	110	Success	Success	Success
BFH Smartshuttle	1	2	110	Success	Success	Success
BFH Smartshuttle	1	3	110	Success	Success	Success
BFH Smartshuttle	2	1	550	Success	Success	Failure
BFH Smartshuttle	2	2	550	Success	Success	Success
BFH Smartshuttle	2	3	550	Success	Failure (knocked cone)	Success
BFH Smartshuttle	3	1	850	Success	Success	Success
BFH Smartshuttle	3	2	850	Success	Success	Success
BFH Smartshuttle	3	3	850	Success	Failure (knocked cone)	Success
BFH Smartshuttle	4	1	1000	Success	Success	Success
BFH Smartshuttle	4	2	1000	Success	Success	Success
BFH Smartshuttle	4	3	1000	Success	Failure (knocked cone)	Success

Table 23: Summary of parking tests BFH Smartshuttle

Summary of parking tests LOXO Alpha

Vehicle	Pass.	Attempt	Latency (ms)	Approach	Parking	Exit
LOXO Alpha	1	1	110	Success	Success	Success
LOXO Alpha	1	2	110	Success	Success	Success
LOXO Alpha	1	3	110	Success	Success	Success
LOXO Alpha	2	1	550	Success	Success	Success
LOXO Alpha	2	2	550	Success	Success	Success
LOXO Alpha	2	3	550	Success	Success	Success
LOXO Alpha	3	1	850	Success	Success	Success
LOXO Alpha	3	2	850	Success	Success	Failure
LOXO Alpha	3	3	850	Failure (knocked cone)	Success	Success
LOXO Alpha	4	1	1000	Success	Success	Success
LOXO Alpha	4	2	1000	Success	Success	Failure
LOXO Alpha	4	3	1000	Success	Failure (knocked cone)	Success

Table 24: Summary of parking tests LOXO Alpha

4.6.2.3 Tests Scenario 8 - false positive obstacle detection

A total of 11 test runs were conducted under the false positive scenario, using two different non-obstacles (branches with leaves and an empty paper bag). The AEB (Automated Emergency Braking) system of both vehicles detected the obstacles in every case, triggering an emergency stop. The Teleoperator then used two different solutions: bypassing the obstacle by moving into the left lane or driving over the obstacle at very low speed (< 1.0 km/h). This setting allows running over the non-obstacle despite the AEB system in principle being active.

As with the parking tests, the assessment was primarily qualitative. While precise vehicle positioning data was recorded, the success of the test depended on whether the vehicle successfully remained within lane boundaries. Both solution approaches were successfully tested for both vehicles. To illustrate both solution routes, still frames from the test videos are shown in Figure 85 and Figure 86. Table 25 contains a summary of all scenario tests.

Summary of scenario tests				
Vehicle	Passage	Attempt	Latency (ms)	Obstacle Avoidance
BFH Smartshuttle	1	1	110	Success
BFH Smartshuttle	1	2	110	Success
BFH Smartshuttle	1	3	110	Success
BFH Smartshuttle	2	1	550	Success
BFH Smartshuttle	2	2	550	Success
BFH Smartshuttle	2	3	550	Success
BFH Smartshuttle	3	1	850	Success
BFH Smartshuttle	3	2	850	Success
BFH Smartshuttle	3	3	850	Success
BFH Smartshuttle	4	1	1000	Success
BFH Smartshuttle	4	2	1000	Success
BFH Smartshuttle	4	3	1000	Success
LOXO Alpha	1	1	110	Success
LOXO Alpha	1	2	110	Success
LOXO Alpha	1	3	110	Success
LOXO Alpha	2	1	550	Success
LOXO Alpha	2	2	550	Success
LOXO Alpha	2	3	550	Success
LOXO Alpha	3	1	850	Success
LOXO Alpha	3	2	850	Success
LOXO Alpha	3	3	850	Success
LOXO Alpha	4	1	1000	Success

Vehicle	Passage	Attempt	Latency (ms)	Obstacle Avoidance
LOXO Alpha	4	2	1000	Success
LOXO Alpha	4	3	1000	Success

Table 25: Summary of scenario tests

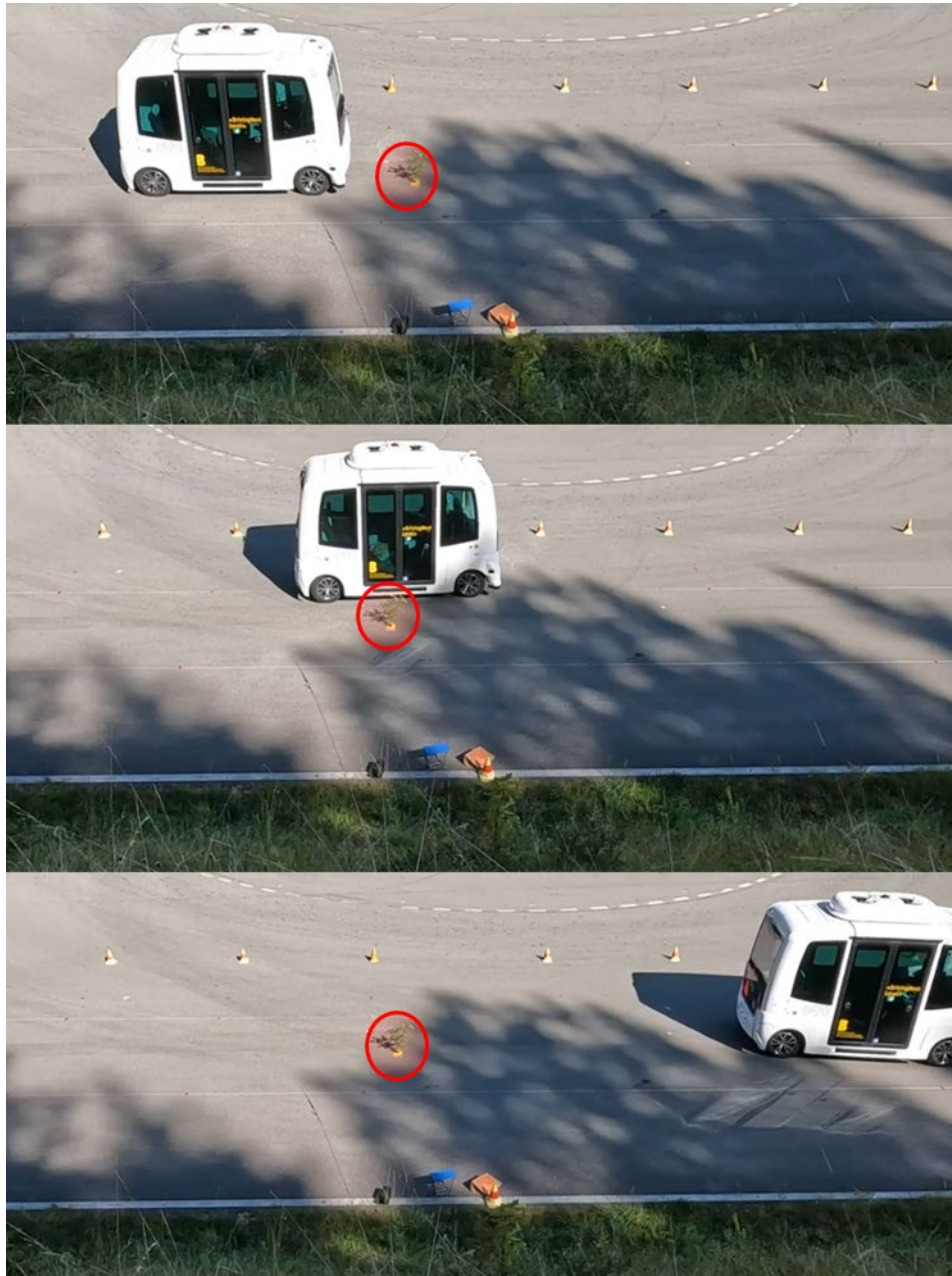


Figure 85: Scenario 8 - "Bypassing" solution in the false positive obstacle detection test

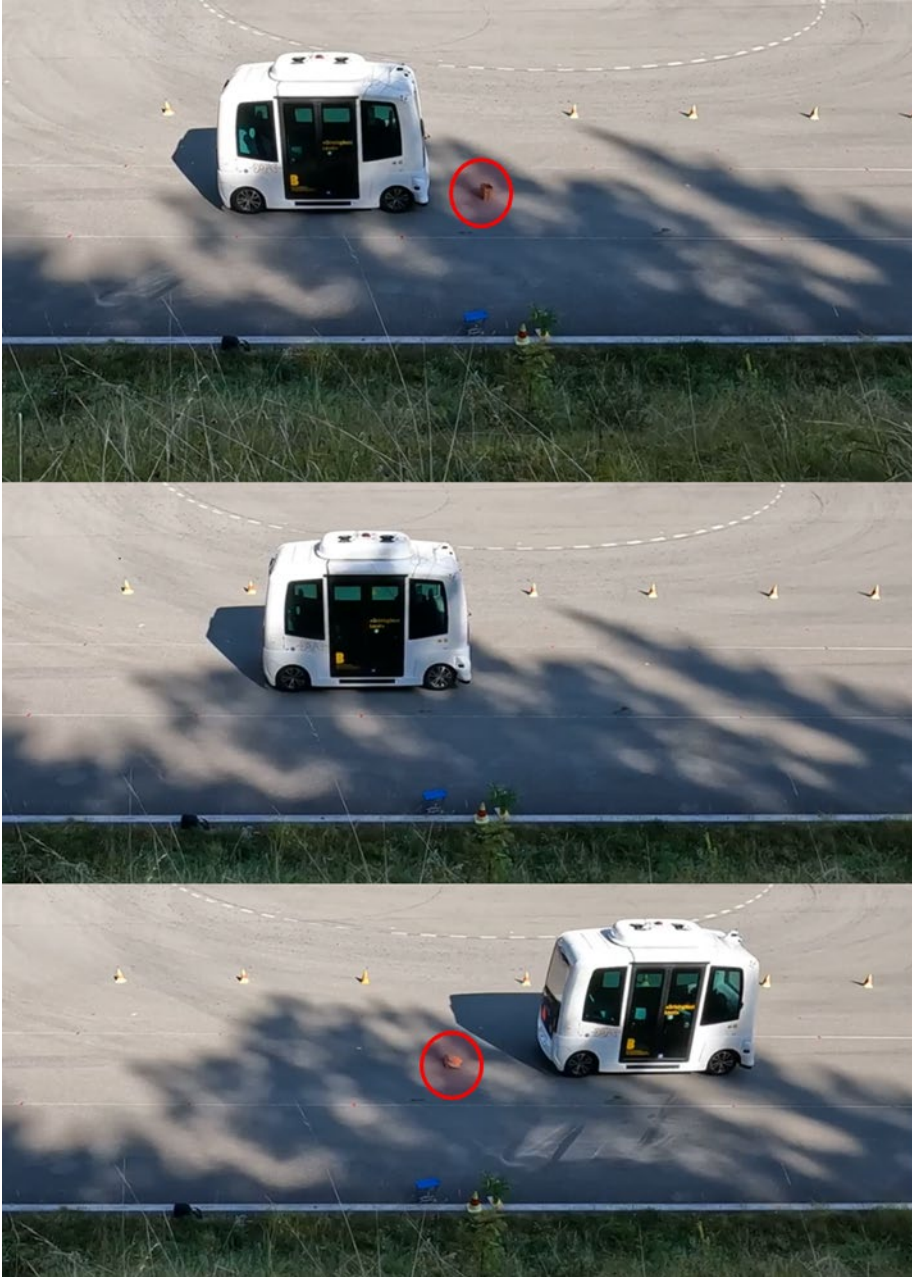


Figure 86: Scenario 8 - "Running over" solution in the false positive obstacle detection test

4.6.3 Discussion and Conclusion

With latencies (glass to glass) of up to 850 ms, the performed **slalom tests** did not show any signs of reduced manoeuvrability, either from Remote Operator feedback or from location recordings. This does not contradict existing studies, although they report influences on driving performance at much lower one-way latencies [74] [72], given that the speeds in the present tests was significantly lower. At a video latency of 1250 ms, an elevated mean distance from mean was observed in the slalom tests. Though not statistically significant with the number of valid tests performed, the limit of manoeuvrability at low speeds can probably be assumed to be in this order of magnitude. This should be investigated with more extensive test series in the future. Nevertheless, keeping in mind the results of the braking distance considerations in 4.5.5.3, it can be concluded that the latency limits as defined in the proposed set of requirements are well within the interval that can be considered safely driveable.

In the **parking tests**, even at video latencies of 1000 ms, no adverse effects of high latencies were observed. This is in line with the conclusion above. While parking manoeuvres generally seem to be a difficult task in Teleoperation (ROL2), latency is likely not a relevant factor.

“**Scenario 8 - False positive obstacle detection**” could be triggered reliably in all tests. This confirms the relevance of the scenario, as it can occur realistically and leads to situations which the AV cannot solve on its own. However, with the existing vehicles and the Remote Operation levels at hand, the Remote Operator managed to reliably solve the Scenario, confirming that the proposed requirements are in principle sufficient for this Scenario. Furthermore, a threshold speed for the activation of the requirements was essential for one of the solution routes. Further discussion is needed to determine whether such a threshold should be implemented in future requirements considering possible additional risks and benefits.

As a conclusion, the working group has agreed on the following points:

- **ROL2 – Teleoperation:** A roundtrip latency of 850 ms enables safe direct operation of the vehicle, since the allowed speed for this level is relatively low (6 km/h), and conform with the tests conducted at the DTC (described in 4.6)
- **ROL3 – Teleassistance Operation L1:** The working group has decided to allow a roundtrip latency of 700 ms, based on various research findings (see ROL3 requirements in 7.1 A1 - List of Minimum Requirements) regarding the effects of latency on remote operation. At this level, the Remote Operator only has access to the vehicle's speed in order to assist the AV in situations that cannot be managed by the automation algorithms (e.g., priority agreement situations)
- **ROL4 – Teleassistance Operation L2 and ROL5 Teleassistance Monitoring:** Latency is no longer considered a minimum requirement. However, a stable network connection is essential to obtain all telemetry information. For these two levels, the Remote Operator no longer has direct control over the automated vehicle. The Remote Operator can only suggest trajectory proposals or communicate with individuals inside or around the AV

4.7 Cybersecurity Tests

4.7.1 Introduction

Various cybersecurity tests were conducted as part of WP4 in this project. These tests served as an extension to the process of validating the cybersecurity requirements for robustness and comprehensiveness for teleoperated driving systems. The requirements, as detailed in chapter 4.4.3, guided the focus areas for validation, ensuring alignment with international standards like ISO 21434 and UNECE Regulation No. 155. As explained in the section 4.5, cybersecurity requirements play a vital role in teleoperated driving. Considering the rapidly evolving digital landscape, it is recognized that achieving a completely secure system is impossible.

4.7.2 Penetration testing approach

The pentest approach is oriented toward some well-known standards in the industry such as the Cyber-Kill Chain [75], MITRE ATT&CK [76], Open Worldwide Application Security Project [77] or International Society of Automation [78]. The assessors use tools associated with manual research and analysis. These tools are as close as possible to what hackers typically use. Some are also developed with custom modules. Metasploit Framework [79] is often used as part of the assessments.

Penetration testing activities can extend over weeks and months if they are not correctly scoped at the beginning of the project. Therefore, the first activity is to scope the penetration testing. In this project, the aim was not to find any generic vulnerabilities present on the vehicles used for the tests, as they do not represent every remote-operated vehicle. Therefore, the tests were scoped to these specific vehicles and would not be relevant for other vehicles. That is why the activities conducted in this project focused only on testing and explaining how some requirements can be tested. The selection of requirements which would be tested was based on a risk assessment made by the pentester and the feasibility of the test given the time constraints and the required expertise.

4.7.3 System Under Consideration

To reduce effort and maximize project output, cybersecurity validation activities were conducted exclusively on one system: the LOXO Alpha 1 vehicle and the related LOXO TCC remote control station. This decision was based on several factors. Firstly, the LOXO Alpha is a complete system developed by LOXO, allowing the team to have full control and hands-on access. This comprehensive access enabled the LOXO team to engage directly with security experts, facilitating detailed discussions about the relevance and effectiveness of the various tests performed. By focusing on this specific system, the project ensured a thorough and efficient validation process. This approach targeted the specific cybersecurity risks of Remote Operation Systems and prioritized threats relevant to the system under consideration.

Hence, the first focus of the present test series was on simulating a threat actor attacking the external, internal, and physical perimeter of LOXO's Alpha vehicle:

- Take control of one of the automated vehicles
- Identify weaknesses in the automated vehicle's security design

4.7.4 Methodology

The first focus of the present test series was on simulating a threat actor attacking the external, internal, and physical perimeter of LOXO's Alpha vehicle. To cover as much of the LOXO's infrastructure as possible, the assessors focused on looking for well-known, exploitable vulnerabilities. Distributed Denial of Service (DDoS) aspects were explicitly excluded from the assessment.

The goal of the assessors was to mimic the attack paths commonly taken by hackers to compromise the infrastructure. The focus was put on the following goals, corresponding the main business risks of LOXO:

- Reach and compromise the Remote Operator Stations
- Take control of one of the AVs
- Identify weaknesses in the AVs security design

4.7.5 Attack Paths

The evaluated attack paths (AP) included various methods to test the security of the system. An attack path refers to the route that a malicious actor might take to infiltrate a target system. This involves bypassing security controls, exploiting vulnerabilities, and escalating privileges to gain access to critical assets within the network. During a pentest, ethical hackers simulate these attack paths to identify and address potential security weaknesses before they can be exploited by real attackers. This helps organizations understand how their systems might be compromised and allows them to strengthen their defenses accordingly. The attack paths studied during the pentests are based on the system under consideration and the methodology.

AP 01 focused on the Remote Operator Station's external perimeter, involving wireless penetration testing to review Wi-Fi security, physical access attempts to TCC devices, and network scanning and enumeration to identify open ports and services for exploitation. AP 02 targeted the internal perimeter of the Remote Operator Station, where internal network scanning helped identify hosts, running services, and open ports, followed by vulnerability analysis and exploits to examine potential security gaps. Additionally, investigations were conducted on potential malware infections, lateral movements within the network, privilege escalation, and data extraction attempts. AP 03 involved both the internal and external perimeters of the vehicle, concentrating on the interception and analysis of internal communications within the vehicle.

4.7.5.1 AP 01 – Remote Operator Station – external perimeter

- Wireless Penetration Testing: Review of Wi-Fi security, attempting to gain access through insecure networks
- Physical Access: Gain physical access to the TCC devices
- Network Scanning and Enumeration: Identification of open ports and services for exploitation

4.7.5.2 AP 02 – Remote Operator Station – internal perimeter:

- Scanning the internal network: Identification of hosts, running services, open ports, and vulnerable systems
- Vulnerability analysis and exploits: Examining identified vulnerabilities for potential exploits and security gaps
- Malware infections and lateral movements: Investigating potential malware infections, lateral movements within the network, privilege escalation, and data extraction attempts

4.7.5.3 AP 03 – Vehicle - internal & external perimeter

- Communication Interception: Interception and analysis of internal communication within the vehicle
- Firmware Manipulation: Attempt to manipulate the vehicle's firmware
- Wireless Penetration Testing: Examination of the vehicle's Wi-Fi security
- Testing signals for external influences: Investigation of the vehicle sensors and communication interfaces for susceptibility to external manipulations or disruptions

4.7.5.4 Limits across all scenarios

The following activities were specifically defined as out-of-scope of the assessment:

- Assessment of physical security measures of the TCC
- Assessment of security of external third-party components in the vehicle
- Long-term monitoring of vehicle communication
- Distributed-Denial-of-Service (DDoS) simulation

The tests were conducted on the automated “Alpha” vehicle and its remote driving station by LOXO.

4.7.6 Cybersecurity Test Results

As this document is intended for public dissemination, detailed test results have been omitted due to the sensitive nature of the information. Instead, the validation of the requirements is summarized in the tables below. It is important to note that certain cybersecurity requirements were not subjected to testing, owing to constraints on resources and the imperative to delineate specific boundaries for the assessment. These limitations were considered, with decisions made based on discussions with LOXO, thereby ensuring that the prioritization of testing efforts was judicious.

The following tables exclusively include the validated cybersecurity requirements. For a comprehensive list of all cybersecurity requirements, please refer to 7.4 A4 – Details Cybersecurity Test .

4.7.6.1 Remote Operator Station

Cybersecurity test results for Remote Operator Station		
ID	Category	Description
CR017	Remote Operator Station	Roles with different responsibilities regarding the TCC (e.g. Administrator, Driver, Hardware Specialist, etc...) shall be defined.
CR022	Remote Operator Station	An inventory of information about TCCs shall be maintained.
CR032	Remote Operator Station	Rules to control physical and logical access to the TCC shall be established.
CR033	Remote Operator Station	Physical entry controls to rooms with TCCs shall be implemented.
CR034	Remote Operator Station	Logical access controls to TCCs shall be implemented.
CR035	Remote Operator Station	Physical and logical access to TCCs shall be logged.
CR036	Remote Operator Station	A specific login-identity shall only be linked to a single person to be able to hold the person accountable for actions performed.
CR038	Remote Operator Station	Non-guessable passwords or PINs shall be enforced.
CR039	Remote Operator Station	Unique passwords or PINs shall be enforced.
CR043	Remote Operator Station	Strong passwords according to best practice recommendations shall be enforced
CR053	Remote Operator Station	Password encryption and hashing shall be performed according to approved cryptographic techniques for passwords.
CR076	Remote Operator Station	TCCs shall be independently reviewed/tested regarding information security.
CR081	Remote Operator Station	TCCs shall include appropriate measures if they can be accessed from remote
CR085	Remote Operator Station	TCCs shall be located in secure areas.
CR086	Remote Operator Station	Rooms with TCCs shall only be accessible after authorisation.
CR087	Remote Operator Station	Access to rooms with TCCs shall be continuously monitored.
CR088	Remote Operator Station	Video Monitoring shall be in places/rooms for locations where TCCs are installed
CR089	Remote Operator Station	Rooms with TCCs shall be equipped with an alarm system.
CR090	Remote Operator Station	TCCs shall not be exposed to environmental threats (e.g. heat, humidity, earthquakes, fire, flooding, etc...)
CR091	Remote Operator Station	TCCs shall not be exposed to physical threats (e.g. hits, theft, vandalism, etc...)
CR092	Remote Operator Station	Rooms with TCCs shall be automatically locked.
CR093	Remote Operator Station	TCCs shall be locked when not in use.
CR094	Remote Operator Station	Screens of TCCs shall not be exposed to shoulder surfing respectively shall not be placed with windows behind the driver's position.
CR105	Remote Operator Station	TCCs shall restrict the installation of software

ID	Category	Description
CR106	Remote Operator Station	TCCs shall receive security updates automatically
CR107	Remote Operator Station	TCCs shall have access controls in place
CR108	Remote Operator Station	Storage devices of TCCs shall be encrypted
CR109	Remote Operator Station	TCCs shall be protected against malware
CR110	Remote Operator Station	It shall be possible to remotely disable, delete or lock out TCCs
CR111	Remote Operator Station	TCCs shall be backed-up regularly.
CR112	Remote Operator Station	TCCs shall be used only for one purpose, hence e.g. web access shall be disabled
CR115	Remote Operator Station	If TCCs do not use WiFi, the WiFi shall be disabled by default
CR116	Remote Operator Station	Users with Privileged Access Rights shall be identified
CR117	Remote Operator Station	Privileged access rights shall be allocated on a event-by-event basis
CR118	Remote Operator Station	Remote drivers shall not have privileged access rights for normal day usage
CR119	Remote Operator Station	All things carried out with an account having privileged access rights shall be logged for audit purposes
CR120	Remote Operator Station	Accounts with privileged access rights shall be linked to one person only.
CR121	Remote Operator Station	TCCs shall not let unauthorized or unknown users have access to sensitive information
CR123	Remote Operator Station	TCCs shall incorporate granular control over who can access what information and applications
CR124	Remote Operator Station	Access to source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled.
CR125	Remote Operator Station	Secure authentication technologies shall be used
CR126	Remote Operator Station	Multi Factor Authentication shall be used
CR127	Remote Operator Station	All log in attempts shall be logged
CR128	Remote Operator Station	Passwords shall not be visible while entering them
CR130	Remote Operator Station	Vulnerabilities of TCCs shall be reduced actively
CR131	Remote Operator Station	Malware detection mechanisms shall be updated regularly
CR132	Remote Operator Station	Technical vulnerabilities shall be managed actively
CR133	Remote Operator Station	Configurations, including security configurations, of TCC-hardware shall be established, documented, implemented, monitored and reviewed.
CR134	Remote Operator Station	Configurations, including security configurations, of TCC-software shall be established, documented, implemented, monitored and reviewed.
CR135	Remote Operator Station	Information stored on TCCs shall be deleted if not used anymore
CR138	Remote Operator Station	TCCs shall be equipped with appropriate Data Loss Prevention

ID	Category	Description
CR141	Remote Operator Station	TCCs shall be monitored continuously
CR142	Remote Operator Station	Networks shall be monitored continuously
CR146	Remote Operator Station	Only specialists shall be allowed to make software changes on TCCs
CR147	Remote Operator Station	Networks and network devices shall be secured to protect information in systems and applications.
CR148	Remote Operator Station	Networks and network devices should be managed to protect information in systems and applications.
CR149	Remote Operator Station	Networks and network devices should be controlled to protect information in systems and applications.
CR150	Remote Operator Station	TCCs shall only connect to authorized networks
CR151	Remote Operator Station	TCCs access to external websites should be managed to reduce exposure to malicious content.
CR152	Remote Operator Station	TCCs shall follow appropriate rules of cryptography
CR153	Remote Operator Station	Appropriate key management for in TCCs or Communication used keys shall be used at any time
CR156	Remote Operator Station	Testing TCCs shall include security testing (e.g. with pen-tests, vulnerability scans)
CR159	Remote Operator Station	TCCs shall be tested in secure environments and setups
CR173	Remote Operator Station	TCC server shall only be accessible from recognized computer
CR174	Remote Operator Station	TCC's network shall be segmented to ensure an isolation of the TCC from non critical systems

Table 26: Cybersecurity test results for Remote Operator Station

4.7.6.2 Remote Vehicle

Cybersecurity test results for Remote Vehicle

ID	Category	Description
CR008	Remote Vehicle	The Remote Vehicle shall have the capability to prevent un-authorized access
CR011	Remote Vehicle	The Remote Vehicle shall implement a unique identification and authentication methodology to ensure the TCC's identity
CR012	Remote Vehicle	The communication channel used for the remote operation shall only be used for remote operations
CR162	Remote Vehicle	The Remote Vehicle shall manage different privilege of authorisation levels
CR165	Remote Vehicle	The Remote Vehicle shall have a secure boot mechanism to avoid any firmware modification
CR168	Remote Vehicle	A security assessment shall be performed to assess risks regarding system interconnections
CR171	Remote Vehicle	The network shall be segmented between critical systems (controls systems) and less critical system (infotainment)
CR172	Remote Vehicle	The Remote Vehicle shall have the capability to react to un-authorized access
CR178	Remote Vehicle	The Remote Vehicle shall implement the least privilege concept between critical and less critical component inside the vehicle

Table 27: Cybersecurity test results for Remote Vehicle

4.7.6.3 Communication

Cybersecurity test results for communications

ID	Category	Description
CR001	Communication	The communication between the vehicle and the TCC shall be authenticated
CR026	Communication	Non-repudiation shall be ensured during communication between vehicle and TCC.
CR029	Communication	The communication service shall be available according to its needs.
CR031	Communication	Communicating with a wrong recipient shall be impossible.

Table 28: Cybersecurity test results for communications

4.7.6.4 Remote Operator

Cybersecurity test results for Remote Operator

ID	Category	Description
CR042	Remote Operator	Strong passwords according to best practice recommendations shall be used
CR113	Remote Operator	User shall log-off once they are not using the TCC anymore

Table 29: Cybersecurity test results for Remote Operator

4.7.7 Discussion and Conclusion

To enhance the security of teleoperated driving systems, it is recommended to put in place a cybersecurity risk management process. It shall include regular attack simulations / penetration testing. It is important to note that while such technical assessments can validate certain requirements listed above, they are not meant to be exhaustive. To uphold and improve the security posture of any Remote Operation System it is imperative to evaluate the system using attack vectors commonly employed by malicious actors, with a particular emphasis on objectives that align with predominant business risks. A thorough debrief of the technical assessment and penetration tests with the developers is essential to meticulously review the report findings. Vulnerabilities must be prioritized based on their severity and potential impact, with critical issues addressed first through a risk-based approach.

Additionally, it is crucial to implement regular security assessments to proactively manage and mitigate emerging cybersecurity threats, thereby identifying new vulnerabilities in a timely manner.

5 Identified Future Research Needs

5.1 Introduction

This section identifies the gaps and challenges that remain unresolved and outlines potential directions for future studies. Addressing these research needs is essential to advance the field and to ensure that Remote Operation Systems can be safely and effectively integrated into broader transportation networks. The findings in this chapter will serve as a foundation for future research efforts, guiding the development of more robust and reliable solutions.

5.2 Identification of Research Gaps

The research conducted in this project highlights several gaps that need further investigation to enable the safe and efficient implementation of automated driving systems. The identified research gaps align closely with the findings of the Teleoperation Research Needs Working Group [80]. These gaps focus on critical areas where improvements in technology, standards, and methodologies are required to overcome current limitations and meet the minimum requirements for Remote Operation Systems. Key research gaps identified include:

- **Efficient Use of Mobile Network Resources:** From the perspective of mobile network operations, optimizing uplink data usage is critical. Camera feeds and other high-bandwidth data streams sent from the remote vehicle to the network should ideally not exceed 10 Mb/s to ensure the scalability of Teleoperation and Teleassistance across a larger fleet. Uplink capacity is a valuable and limited resource within mobile networks, necessitating careful allocation among all remotely monitored or controlled vehicles. Moreover, high-bitrate streams should be transmitted selectively—only when the Remote Operator needs to observe the vehicle’s surroundings (e.g., in ROL 3, 4, or 5) or take direct control of the vehicle (e.g. in ROL 2). Research is needed to explore adaptive data streaming strategies and dynamic resource allocation techniques to address these challenges effectively.
- **Safety-Critical Remote Operator Workplace:** The current HMIs used in Remote Operation Systems face challenges in conveying essential information to the Remote Operator quickly and accurately. There is a need for further research into optimizing HMI designs to enhance Remote Operator situational awareness, including better visual feedback, ergonomic controls, and intuitive interfaces that can reduce cognitive workload and improve response times.
- **Fleet management 24/7:** In order to guarantee the secure operation of a Remote Operation System 24/7 for monitoring and controlling an entire fleet of AVs, it is necessary to scale up from a single Remote Operator Station to a Remote Operation System that allows several Remote Operators to carry out several

interventions in parallel. It is therefore likely that this will also require a division of roles, as is common in other areas, so that the Remote Operation System can provide an overview of the entire fleet and a team with different responsibilities can divide up the tasks.

- **Operational Design Domain Limitations and Scenarios:**

The ability to extend the defined scenarios and ODD boundaries for Remote Operation Systems remains limited by current technological capabilities and legal frameworks. Additional research is necessary to develop more flexible ODD definitions and incorporate a broader range of scenarios to account for complex urban environments and cross-border operations.

- **Personnel Training and Emergency Management:**

Ensuring that Remote Operators are well-trained to handle unexpected situations remains a challenge. Research is needed to establish standardized training programs, including the use of simulations for emergency scenarios, to better prepare Remote Operators for real-world conditions in Teleassistance (ROL3-5) and Teleoperation (ROL2).

- **Technological Challenges in Teleoperation (ROL2):**

While advancements in technologies for Remote Operation Systems have enabled Teleassistance and Direct Control of AVs, there are still significant challenges associated with stable connections between the Remote Operation Centre and the AV. Research is needed to improve communication redundancy and latency management to ensure reliable operation under various environmental and operational conditions.

- **Standardization and Alignment with International Norms:**

The lack of universally accepted standards for Teleoperation and Teleassistance, especially in the context of integrating various Remote Operation Levels (ROLs) and functionalities, presents a significant barrier. This project has identified overlaps between the requirements defined here and existing standards such as **UN Regulation No. 46** and **ISO 16505:2019** for camera monitor systems, particularly regarding system latency, image formation time, and frame rates. Further alignment with these standards and periodic reviews to update requirements are crucial for ensuring safety and interoperability.

Additionally, the relevance of other regulations such as UN Regulation No. 157 (approval of vehicles with regards to Automated Lane Keeping Systems ALKS), EU Regulation 2019/2144, and implementing Regulation EU 2022/1426 highlights the need for further research to ensure compliance and interoperability. Planned revisions to the Swiss SVG for automated driving should also be considered as part of future research efforts.

These research gaps emphasize the need for a coordinated approach to advancing Teleoperation and Teleassistance technologies, integrating findings from both national and international research efforts to address the evolving requirements of the industry. The project's outcomes aim to provide a foundation for future regulatory initiatives and standardization efforts that will facilitate the safe deployment of teleoperated systems on public roads in Switzerland.

5.3 Technical Report of the Working Group BAST

In Germany, a working group „**Research Needs in Teleoperation**“, consisting of 38 (mainly scientific) experts, published an important report [80] as part of a research project coordinated by the “Bundesamt für Strassenwesen” (BAST). The report provides a comprehensive overview of the outstanding questions and unresolved issues that must be addressed to ensure the successful integration of Teleoperation technologies into public roadways. By cross-referencing these findings, this section highlights the areas where further research is most urgently needed and proposes potential pathways for future studies.

The problem definition and approach for this project was:

- Teleoperation as an innovation in road transport
- Usable, safe and efficient integration into existing traffic
- Identifying and structuring research needs at an early stage
- Structuring of research needs in 5+ clusters
- Cross-cluster research questions
- Identifying research questions categorised according to time prioritisation

Figure 87 below shows the five different clusters of this project, three of which include the “**Technical requirements**” block and thus thematically correspond to this project.

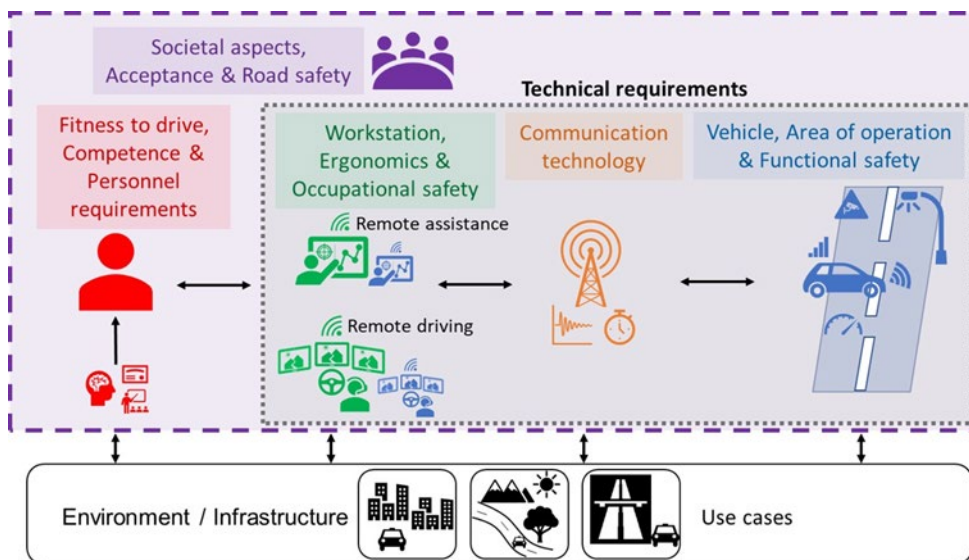


Figure 87: Teleoperation diagram from BAST Report [80]

In this BAST report, a total of 174 cluster-specific and cross-cluster open research questions are identified (Chapter 4). To prioritise these research questions according to their relevance for this research project, the focus is placed on topics that are directly related to this project's objectives and the requirements for the Remote Operation System, particularly with regard to:

- System reliability and continuous operation (24/7 operation)
- Extension of the defined scenarios and use cases (ODDs and infrastructure requirements)
- Basis for future tenders and minimum requirements (e.g. for the ASTRA MB4 working group)

Table 30 includes the priority for each research question based on their relevance to this project's goals and objectives:

- **Highest Priority** (Directly relevant for 24/7 operation and extending scenarios): Questions about latency, communication quality, system architecture, and safety measures
- **Medium Priority** (Important for scenario expansion and potential future calls for proposals): ODDs, simulation tools, integration issues, cybersecurity
- **Lower Priority** (Relevant for further research approaches and long-term calls for proposals): Potential for new business models, social acceptance, and the role of human operators

Relevant Research questions from BAST Report

Research Question	Justification	Reference	Prio
What are the maximum tolerable latency and jitter levels in communication systems used for Teleoperation, considering human factors?	Determines communication requirements, essential for minimizing latency and ensuring reliable operation.	Cluster 3, Chapter 4.3.4	High
How can latency and jitter limits be empirically validated?	Provides a foundation for empirically validating critical performance parameters.	Cluster 3, Chapter 4.3.4	High
What quality parameters are necessary for network availability and communication requirements?	Defines network and communication requirements to support uninterrupted operation.	Cluster 3, Chapter 4.3.4	High
Can Teleoperation functions be distributed across subsystems or centralized, and what architectural frameworks support these configurations?	Addresses system architecture concerns critical for 24/7 operation and reliability.	Cluster 1, Chapter 4.1.3	High
What technical measures ensure a risk-minimized state for teleoperated vehicles?	Identifies safety measures necessary for secure Teleoperation system deployment.	Cluster 1, Chapter 4.1.5	High
How can Operational Design Domains (ODDs) be extended for Teleoperation where automated driving alone is insufficient?	Ensures that ODDs are suitable for Teleoperation, expanding the range of applicable scenarios.	Cluster 1, Chapter 4.1.1	Medium
What simulation tools and scenario databases are needed to research Teleoperation driving situations?	Identifies tools and databases needed for thorough scenario analysis.	Cluster 4, Chapter 4.4.4	Medium

Research Question	Justification	Reference	Prio
How should interfaces between Teleoperation systems and other transport systems be designed for seamless intermodal integration?	Focuses on integration of Teleoperation with other transport systems, relevant for extending scenarios.	Cluster 1, Chapter 4.1.3	Medium
What cybersecurity measures are needed to protect Teleoperation systems from attacks?	Focuses on security measures critical for protecting data and maintaining system integrity.	Cluster 3, Chapter 4.3.7	Medium
Are new approaches needed for hazard identification and risk assessment in Teleoperation?	Explores new methods for risk management, vital for system safety and reliability.	Cluster 1, Chapter 4.1.5	Medium
How can Teleoperation assistance be modelled and simulated in virtual environments?	Enables development of virtual environments for safe and cost-effective testing.	Cluster 4, Chapter 4.4.4	Medium
To what extent is Teleoperation a bridging technology for current limitations in automated driving?	Assesses Teleoperation's role in overcoming current technological barriers in automated driving.	Cluster 1, Chapter 4.1.1	Medium
What are the requirements for creating ad-hoc networks for mobility data sharing between cities and municipalities?	Supports understanding of requirements for communication and data sharing, key for reliable operation.	Cluster 3, Chapter 4.3.5	Medium
What potential does Teleoperation have to enable new business models, such as car-sharing?	Explores new business opportunities enabled by Teleoperation, supporting economic viability.	Cluster 5, Chapter 4.5.3	Low
What is the role of digital twins in Teleoperation architectures?	Explores potential new technologies (digital twins) for enhancing Teleoperation systems.	Cluster 1, Chapter 4.1.2	Low
What factors influence the acceptance of Teleoperation technologies by users and society?	Enhances understanding of social acceptance, important for regulatory approvals.	Cluster 5, Chapter 4.5.3	Low
Does a human Remote Operator increase acceptance of automated systems?	Investigates the role of human operators, relevant for mixed-mode operation scenarios.	Cluster 5, Chapter 4.5.3	Low
How can different types of cyber-attacks on Teleoperation systems be classified?	Analyses potential threats, providing a framework for comprehensive cybersecurity strategies.	Cluster 3, Chapter 4.3.7	Low

Table 30: Relevant Research questions from BAST Report [80]

5.4 Recommendations and Prerequisites

The successful development and deployment of Remote Operation Systems for automated vehicles (AVs) require a comprehensive approach that balances technological innovation, regulatory compliance, cybersecurity resilience, and operational safety. The following recommendations and prerequisites are derived from the project's findings and are structured to address key areas critical for the advancement of Teleoperation and Teleassistance technologies.

5.4.1 Focus on Safety as a fundamental principle

Ensuring the safety of all road users and vehicle occupants is crucial for the safe implementation of teleoperated driving. A high level of safety is required in order to be able to intervene in driving operations at any time. Safety includes both technical aspects (e.g. a stable connection between the vehicle and the control centre) and regulatory requirements (e.g. compliance with traffic regulations and safety standards). Cybersecurity is an integral part of safety, as vulnerabilities in communication channels or system integrity could compromise overall safety. Regular cybersecurity assessments and updates are essential to maintain resilience against evolving threats.

5.4.2 Refinement and Expansion of Scenario Definitions

Continuous updates to scenario definitions are essential, incorporating insights gained from real-world applications. In addition to refining existing scenarios, it is crucial to develop new ones that address emerging operational challenges, such as higher vehicle speeds, complex urban environments, and adverse weather conditions. This approach ensures the scenarios remain comprehensive and aligned with the evolving demands of Remote Operation Systems.

5.4.3 Technological Development and Adaptation to New Standards

As teleoperated driving and automated driving are still relatively new technologies, continuous progress is expected in the coming years. In order to keep pace with technological developments, the defined requirement criteria should be regularly reviewed and adapted. Both technological innovations and changes in the relevant regulations and standards must be taken into account. Practical experience could also provide valuable insights to further optimize the criteria.

The following areas have been identified as critical for technological advancement and should be prioritized in the development and adaptation of Remote Operation Systems:

1. Adaptive Data Streaming and Resource Optimization

As teleoperated systems scale to support larger fleets, efficient use of uplink bandwidth becomes critical. Developing adaptive data streaming strategies can ensure that high-bandwidth streams, such as camera feeds, are prioritized only when necessary (e.g., during Teleoperation in ROL2). Additionally, dynamic resource allocation techniques are needed to balance communication loads across fleets, maintaining reliability while optimizing network resource usage. These approaches will enhance scalability and enable robust operations even under high network traffic conditions. The feasibility of teleoperated driving in current mobile networks has been evaluated in [81], demonstrating the challenges of variable latency and bandwidth availability. Furthermore, the study [82] presented an approach to reduce the bandwidth requirements for mobile networks through optimized data rate reduction techniques. This approach was validated by measurements and a user study, highlighting its potential to enhance the scalability and efficiency of Remote Operation Systems.

2. Multimodal Feedback Mechanisms

The inclusion of multimodal feedback mechanisms in Remote Operation Systems is increasingly recognized as a critical factor for safety and operator performance. Research has shown that providing Remote Operators with predictive haptic and visual feedback can improve both situational awareness and control accuracy. For example:

- Predictive haptic feedback mechanisms for lateral control enhance steering precision in urban scenarios [83] [84]
- High-quality video streams significantly improve the ability of Remote Operators to avoid obstacles and respond to dynamic challenges in real time [85]

Integrating these advancements into development strategies will ensure optimal operator performance in diverse scenarios.

3. Cybersecurity and System Resilience

Resilient communication systems, secured against potential cyber threats, are essential to ensure reliable system performance and data integrity. The integration of state-of-the-art cybersecurity technologies, along with regular penetration testing, should be prioritized to safeguard these systems.

4. Insights from Related Research

The research project “Auswirkungen des automatisierten Fahrens” [57] [86] underscores the critical need for continuous development of technological and regulatory standards, especially in mixed traffic scenarios [58]. The project findings demonstrate the central role of data management, data protection and cybersecurity [59].

5.4.4 Refinements for Teleoperation (ROL2)

Teleoperation, i.e. the Direct Control of an automated vehicle by a Remote Operator acting as a Remote Driver in ROL2, must be designed in such a way that the Remote Operator can intervene in driving operations in the event of an emergency or unforeseeable events. This ability to intervene is particularly important when automated driving reaches its technical limits or when unexpected situations occur and cannot be handled by Teleassistance (ROL3-ROL5). Specific refinements for ROL2 operations are required to ensure seamless intervention at low speeds (≤ 6 km/h). Research should focus on:

- **High availability and reliability** of the Remote Operation System to ensure safe intervention at all times
- **Stable and redundant communication channels** between the AV and the Remote Operation Centre to maintain the connection even in the event of technical problems
- **Studying latency effects** in more detail, including the impact of varying latencies on operational responsiveness and precision.
- **Improving Remote Operator interfaces** to facilitate intuitive and efficient control in critical scenarios.
- **Ensuring robust cybersecurity** measures to safeguard communication links and system reliability during ROL2 operations.

Latency continues to be a critical factor influencing the overall effectiveness of Remote Operation Systems. Studies such as [87] and [88] underline the necessity of developing systems capable of mitigating latency-related challenges to enhance both operator performance and system safety.

The importance of real-time visual information and its impact on operator performance is highlighted in [89], which demonstrates how video quality significantly influences operator reaction times and the ability to avoid dynamic obstacles. Ensuring high-resolution, low-latency video streams is therefore a critical component of safe and effective Teleoperation and Teleassistance. Complementing this, [88] provides valuable guidelines for Remote Operation Station interfaces for automated vehicle, offering insights into addressing human factors and usability challenges critical for effective remote operation. Moreover, this topic was the focus of a visit by

representatives of SwissMoves (HEIA-FR, HEG-FR) and LOXO to the German Aerospace Centre (DLR) in February 2024 [90]. The visit facilitated an intensive exchange on the requirements for Remote Operation Centres and the role of Human Factors in ensuring operational efficiency and safety. This collaboration highlighted the growing importance of cross-institutional expertise in refining Remote Operation Systems, particularly in addressing challenges related to user interfaces and operator usability.

5.4.5 Periodic Review and Further Development

As technologies, standards and regulations are constantly evolving, the requirements for teleoperated driving should be reviewed at regular intervals. This review ensures that:

- New technological possibilities can be integrated
- Legal and normative changes are taken into account
- Practical experience and safety-relevant findings contribute to the improvement of the systems
- In-depth cybersecurity training to equip operators with the knowledge and skills to identify and mitigate potential cyber threats during operations

5.4.6 Training and Certification for Remote Operators

The Remote Operators responsible for Teleoperation and Teleassistance must be comprehensively trained and prepared for unforeseen events. This includes:

- Regular training on the technologies used
- Simulation of emergency situations to ensure fast and safe reactions
- Familiarity with applicable traffic rules and regulations in order to be able to act safely in the event of an incident

5.4.7 Alignment with International Standards

The advent of remote-controlled AV's requires that existing standards be adapted. The working group has found substantial overlap between the established requirements and the stipulations of the Regulation No 46 of the Economic Commission for Europe of the United Nations (UNECE) [91] and ISO 16505:2019 [92]. In addition to these, UN Regulation No. 157 (approval of vehicles with regards to Automated Lane Keeping Systems ALKS) and EU Regulation 2019/2144, along with implementing Regulation EU 2022/1426, provide critical frameworks for future standardization efforts. Cybersecurity resilience must also be a critical component of international standardization efforts, ensuring interoperability and alignment with global benchmarks such as ISO/IEC 27001 and UN Regulation No. 155. Incorporating these into research initiatives can not only facilitate alignment with both EU and international regulatory requirements but also enhance system robustness against evolving threats.

These parallels underscore the critical role these standards play in guaranteeing the safety and dependability of remote-controlled driving systems. In particular, for the following sections:

- ISO 16505:2019 - 6.9.1 Frame rate/ UN Regulation No. 46 – 6.2.2.3.4.1 Frame rate: Movements of objects in front of the camera shall be rendered smooth and fluid. The minimum frame rate of the system (update rate of the image information) shall be at least 30 Hz. At low light conditions or while manoeuvring at low speed, the minimum frame rate of the system (i.e. update rate of the image information) shall be at least 15 Hz.
- ISO 16505:2019 - 6.9.2 Image formation time / UN Regulation No. 46 – 6.2.2.3.4.2 Image formation time: The image formation time of the monitor should be less than 55 ms at room temperature $22\text{ }^{\circ}\text{C} \pm 5\text{ }^{\circ}\text{C}$.
- ISO 16505:2019 - 6.9.3 System latency / UN Regulation No. 46 – 6.2.2.3.4.3 System latency: A CMS shall have a sufficient short latency in order to render the scenery nearly at the same time. The latency shall be lower than 200 ms at room temperature $22\text{ }^{\circ}\text{C} \pm 5\text{ }^{\circ}\text{C}$.
- UN Regulation No. 46 – 6.2.1.3 General requirements: System latency: The effectiveness of the CMS of Classes I to IV shall not be adversely affected by magnetic or electrical fields. This shall be demonstrated by compliance with the technical requirements and transitional provisions of Regulation No. 10, 04 series of amendments or any later series of amendments.
- UN Regulation No. 46 – 6.2.2.2.1 Functional requirements for camera-monitor devices of Classes V and VI: The camera shall function well in conditions in which sunlight falls on the camera. The saturated area, defined as the area in which the luminance contrast ratio ($C=L_w/L_b$) of a high contrast pattern falls below 2.0, shall not cover more than 15 per cent of the displayed image under the conditions of paragraphs 6.2.2.2.1.1. to 6.2.2.2.1.4.
- UN Regulation No. 46 – 6.2.2.2.1.2 Functional requirements for camera-monitor devices of Classes V and VI: The camera shall be hit by a (simulated sun) light of 40 klx, spanning an angle between 0.6 and 0.9° with an elevation angle of 10° (directly or indirectly via a mirror) removed from the optical axis of the sensor.
- UN Regulation No. 46 – 6.2.2.2.2 Functional requirements for camera-monitor devices of Classes V and VI: The monitor shall render a minimum contrast under various light conditions as specified by ISO 15008:2017.
- UN Regulation No. 46 – 6.2.2.2.3 Functional requirements for camera-monitor devices of Classes V and VI: It shall be possible to adjust the average luminance of the monitor either manually or automatically to the ambient conditions.
- UN Regulation No. 46 – 6.2.2.2.4 Functional requirements for camera-monitor devices of Classes V and VI: The measurements for the luminance contrast of the monitor shall be carried out according to ISO 15008:2017.
- UN Regulation No. 46 – 6.2.2.3.2 Operating readiness (System availability): If the system is not operational (e.g. CMS failure), it shall be indicated to the driver by i.e. warning indication, display information, absence of status indicator. The operator's manual shall explain the information indicated.
- UN Regulation No. 46 – 6.2.2.3.3.2.1 Day condition with diffuse sky-light exposure test: For the day condition with diffuse sky-light exposure, the test method given in ISO 16505:2015, subclause 7.8.2., Test 2 shall be applied, but a value of 4,000 to 4,200 cd/m² for luminance diffuse illuminator shall be used.

- UN Regulation No. 46 – 6.2.2.3.3.3 Grey scale rendering: A CMS shall have a sufficient grey scale rendering. CMS shall display a tonal range of at least eight distinguishable different grey tonal steps on the monitor.
- UN Regulation No. 46 – 6.2.2.3.3.4 Colour rendering: For colour rendering, the hue angle of reproduced colour of the chart patches on the monitor shall satisfy the following requirements. The colour coordinates are described based in the CIE 1976 uniform colour space:
 - (a) Red colour coordinates shall not exceed the range of (0°, 44.8°) or (332.2°, 360°)
 - (b) Green colour coordinates shall not exceed the range of (96.6°, 179.9°)
 - (c) Blue colour coordinates shall not exceed the range of (209.9°, 302.2°)
 - (d) Yellow colour coordinates shall not exceed the range of (44.8°, 96.6°)
 - (e) To distinguish from the white colour, define distance from white as $R_i \geq 0.02$, where R_i is the chromatic distance of each colour patch ($i = \text{Red, Green, Blue, Yellow}$), relative to white ($i = \text{White}$)
- UN Regulation No. 46 – 6.2.2.3.3.6.2 Depth of field: The CMS shall enable the driver to observe the occupied space by the object and perceive the content shown within the range of interest with detailed resolution.
- UN Regulation No. 46 – 6.2.2.3.3.8.1 Flicker: The entire image area of the monitor shall be free of flicker according to the test method of Annex 12, paragraph 1.2.

Furthermore, the working group recommends a thorough re-evaluation of Articles 5.2.1.3, 5.2.2.3, and 5.2.3.3 of UN Regulation No. 152. In particular, the speed range for the Advanced Emergency Braking System (AEBS) should be adjusted for ROL2 to enable activation at speeds as low as 1 km/h. This modification would create a critical buffer zone (between 0 km/h and 1 km/h), allowing for remote intervention to unblock the vehicle if it encounters an obstruction in its path. Such a change would enhance operational flexibility and safety in various scenarios.

5.4.8 Summary

Clear and **regularly updated minimum requirements** are essential to support the continuous development of the technology enabling Teleoperation (ROL2) and Teleassistance (ROL3-ROL5). Ensuring the safety of all road users and vehicle occupants remains the top priority. This includes both technical innovations, such as stable and redundant communication channels and real-time transmission of vehicle data, and adherence to evolving regulations and safety standards. Regular reviews and updates of these requirements are necessary to integrate new technological advancements, adapt to changes in legal frameworks, and incorporate practical insights gained from real-world operations.

Comprehensive **training for Remote Operators** is another critical factor in ensuring system reliability and safety. Remote Operators, responsible for Teleoperation and Teleassistance, must receive comprehensive training to ensure they can respond swiftly and safely in emergency situations. Training programs should focus on both technical expertise and operational readiness, forming a key component of the Remote Operation Systems overall reliability and robustness.

The research gaps identified by this project closely align with the findings presented in the final report by the “Teleoperation Research Needs” Working Group [80]. This alignment highlights the importance of advancing regulatory frameworks, technological capabilities, and safety standards. As Teleoperation and Teleassistance technologies evolve, it is crucial that national and international standards adapt to meet the increasing demands for safety, reliability, and operational efficiency.

The key recommendations derived from this project are summarized below.

Summary recommendations

Recommendation	Description
1 Focus on Safety as a fundamental principle	Prioritize safety in all technological developments, operational strategies, and regulatory updates.
2 Refinement and Expansion of Scenario Definitions	Regularly update and expand scenario definitions based on real-world insights and emerging challenges.
3 Technological development and adaptation to new standards	Enhance system capabilities through advances in communication technologies and alignment with evolving standards.
5 Periodic review and further development	Continuously reassess and refine requirements to reflect technological progress and regulatory changes.
6 Training and Certification for Remote Operators	Implement comprehensive training programs and certification standards for Remote Operators.
7 Alignment with International Standards	Ensure consistency and scalability by aligning with key international standards, such as ISO and UNECE regulations.

Table 31: Summary recommendations

6 Conclusion

The set of minimal requirements to remotely drive AVs proposed in the present project is based on existing regulations and own research. These requirements encompass technical, operational, and cybersecurity aspects, supported by a **newly developed Taxonomy for Remote Operation Levels (ROLs)** tailored to address key operational scenarios. This set of requirements serves as a foundational draft for the implementation of legal frameworks. However, it represents a snapshot of current technological capabilities in a rapidly evolving field and will require periodic updates to adapt to advancements, changing standards, and evolving regulations.

The project also tackled several open research questions, including **Scenario** validation, the refinement and expansion of Scenario definitions, **cybersecurity** challenges, and the impact of **latency** under varying operational conditions. These efforts highlighted the importance of aligning requirements with international standards and adapting them to technological and regulatory changes. The identified relevant scenarios and **ROLs** proved instrumental for the development and validation of the set of requirements. For example, the "False Positive Obstacle Detection" scenario was replicated and solved experimentally, demonstrating the practicality and relevance of the proposed requirements. Future research should expand on such scenarios to enhance their relevance and applicability. Network latencies were determined to be less critical than expected at the low speeds permitted under ROL2, where the maximum vehicle speed is limited to 6 km/h.

Despite these advancements, certain **challenges** remain unresolved. Key priorities include refining system performance under varied operating conditions, addressing urban complexities, and ensuring seamless integration into dynamic and international regulatory frameworks. This project focused exclusively on the remote operation of AVs on public roadways within Switzerland. Specific areas such as applications on private property, cross-border monitoring, on-site interventions and the operation of robots on pedestrian paths were deliberately excluded from the scope but should be addressed by future research.

A Remote Operation System cannot be considered safe until its **cybersecurity resilience** has been proven. Thus, this project highlighted the cybersecurity requirements, emphasizing their critical role in protecting communication channels, data integrity, and system reliability against evolving threats. Regular penetration testing and continuous monitoring of cybersecurity measures are essential to ensure state-of-the-art resilience in Remote Operation Systems.

Recommendations for Governance and Future Development

It is recommended to establish a comprehensive governance and management framework to oversee the implementation and ongoing evaluation of Swiss requirements to remotely drive automated vehicles. This framework should define roles, responsibilities, and processes for continuous improvement, including mechanisms for adapting to regulatory changes and integrating new technological developments. By addressing key provisions outlined in Chapter 5 of the OCA/VAF ordinance [5], the project provides a robust foundation for such a framework. The establishment of a framework will ensure that the requirements remain robust, actionable, and aligned with national and international standards.

Leveraging its extensive expertise and insights, the consortium is well-positioned to actively support this governance framework. It could serve as an advisory and operational body, providing guidance on compliance with the OCA/VAF ordinance [5], conducting independent evaluations of adherence to the requirements, and ensuring a robust approval process for Remote Operation Systems.

The developed Terminology and Taxonomy, particularly the structured understanding of Remote Operation Levels (ROLs), are invaluable tools aligning operational practices with the new OCA/VAF ordinance [5] and enabling compliant operations. These efforts contribute to the seamless integration of AVs into Switzerland's public road networks.

Final Remarks

Teleoperation and Teleassistance bridges the gap between manual and fully automated driving, serving as a critical enabling technology for the transition to automated mobility. It facilitates the closure of operational gaps in the deployment and use of autonomous vehicles, particularly in scenarios where full automation may not yet be feasible. This project has established a robust foundation for advancing teleoperated systems, paving the way for their safe, reliable, and efficient integration into modern transportation networks. Continued collaboration between regulatory authorities, industry stakeholders, and research institutions will be vital for realizing this vision.

7 Appendix

7.1 A1 - List of Minimum Requirements

See Table 13 for the description of the requirements list.

7.1.1 Requirements Remote Operation Level (ROL)

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RROLO10	Remote Operator	Operational	ROL2	The Remote Operator shall be responsible for the following tasks: - Maintaining full control over the vehicle. - Performing duties equivalent to those of a normal driver. - Ensuring continuous and effective communication with passengers.	Norm	OCA Art.33 (2)
RROLO20	Remote Operator	Operational	ROL2	The Remote Operator shall be responsible for all Dynamic Driving Task (DDT).	Own experience	
RROLO30	Remote Operator	Operational	ROL2	The Remote Operator shall be responsible for all Object and event detection and response (OEDR).	Own experience	
RROLO40	Remote Vehicle	Operational	ROL2	The systems required to be active in support of the Remote Operator shall include: - Automatic Emergency Braking (AEB) system. - MRM based on network latency and data performance	Own experience	
RROLO50	Remote Operator	Operational	ROL2	During ROL2, the Remote Operator shall maintain ultimate responsibility for the safe operation of the Remote Vehicle.	Own experience	
RROLO60	Remote Operator	Operational	ROL2, ROL3,	The Remote Operator shall be located within Swiss territory.	Norm	OCA Art.33 (1)

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
			ROL4, ROL5			
RROLO70	Remote Vehicle	Operational	ROL2	During ROL2, the maximum speed of the Remote Vehicle shall not exceed 6 km/h.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L221/18 Art. 10
RROLO80	Communication	Performance	ROL2	During ROL2, the roundtrip latency (from AV camera to remote operation centre and from remote operation centre to AV actuators) shall be less than 850 ms.	Own experience	Confirmed by tests done at DTC
RROLO90	Remote Vehicle	Operational	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall undergo a daily routine remote driving check before it operates.	Norm	OCA Art.32 (2)
RROLO100	Remote Vehicle	Operational	ROL2	To enter in ROL 2, the following initial states shall be respected : - Minimal Risk Condition (MRC), speed set to 0 km/h - Stationary brake activated.	Own experience	
RROLO110	Remote Operator Station	Operational	ROL2	To enter in ROL 2, the following initial conditions shall be respected : - Operator brake pedal pushed - Video and Data latency below limit latency - Visibility sufficient - Operating mode awareness	Own experience	
RROLO120	Remote Operator Station	Functional	ROL2	To operate in ROL 2, the Remote Operator Station shall be able to continuously monitor data and video latency.	Own experience	

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RROL130	Remote Vehicle	Operational	ROL2, ROL3, ROL4, ROL5	If operating conditions are not respected, Minimal Risk Manoeuvre (MRM) shall be initiated to achieve a Minimal Risk Condition (MRC) which is a stable, stopped state. The Remote Vehicle shall warn the Remote Operator.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L221/13 Art. 3.1.5
RROL140	Remote Vehicle	Operational	ROL2	To exit ROL 2, the following final states shall be respected : - Minimal Risk Condition (MRC) shall be reached, speed set to 0 km/h - Stationary brake activated.	Own experience	
RROL150	Remote Operator	Operational	ROL3	The Remote Operator shall be responsible for the following tasks: - Path drawing: Mapping out the trajectory and route for the vehicle's movement. - Speed control: Monitoring and adjusting the vehicle's velocity as necessary to ensure safe and efficient operation. - Signalling: Activating appropriate signals and indicators to communicate intentions and actions to other road users. - Communication: Maintaining clear and continuous communication channels with relevant parties involved in the operation.	Own experience	
RROL160	Remote Vehicle	Operational	ROL3	The Remote Vehicle shall be responsible for all Dynamic Driving Task (DDT) except for speed control, which falls under the responsibility of the Remote Operator.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L221/5 Art. 25
RROL170	Remote Vehicle	Operational	ROL3, ROL4, ROL5	The Remote Vehicle shall be responsible for all Object and event detection and response (OEDR).	Own experience	

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RROL180	Remote Vehicle	Operational	ROL3, ROL4, ROL5	During Tele Assistance Operation L1, L2 and monitoring, the Remote Vehicle shall retain ultimate responsibility for safe operation, overseen by the Remote Operator.	Own experience	
RROL190	Remote Vehicle	Operational	ROL3, ROL4, ROL5	During Tele Assistance Operation L1, L2 and monitoring, the maximum speed of the Remote Vehicle shall not exceed road limitation.	Own experience	
RROL200	Communication	Performance	ROL3	During ROL 3, the roundtrip latency (from AV camera to remote operation centre and from remote operation centre to AV actuators) shall be less than 700 ms.	Studies	Teleoperation; Stefan Neumeier et al. Teleoperation of On-Road Vehicles via Immersive Telepresence Using Off-the-shelf Components; Xiaotong Shen et al.
RROL210	Remote Vehicle	Operational	ROL3	To enter in ROL 3, the following initial states shall be respected : - Speed set to 0 km/h.	Own experience	
RROL220	Remote Operator Station	Operational	ROL3, ROL4, ROL5	To enter and operate in ROL 3 to ROL 5, the following operating conditions shall be respected : - Advanced Driving Systems (ADS) shall be operational; - Remote Operator is responsible for ensuring sufficient visibility in order to complete safely remote operation tasks; - Video and/or Data performance below limit value; - The Remote Operator shall be aware of the operating mode.	Own experience	

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RROL230	Remote Operator	Operational	ROL4	The Remote Operator shall be responsible for the following tasks: - Path drawing: Mapping out the trajectory and route for the vehicle's movement. - Path confirmation: Verifying the accuracy and suitability of the planned path before execution, ensuring alignment with safety and operational requirements. - Communication: Maintaining clear and continuous communication channels with relevant parties involved in the operation.	Own experience	
RROL240	Remote Vehicle	Operational	ROL4, ROL5	The Remote Vehicle shall be responsible for all Dynamic Driving Task (DDT).	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L221/5 Art. 25
RROL250	Remote Operator	Operational	ROL5	The Remote Operator shall be responsible for the following tasks: - Supervision: Overseeing the operation of the vehicle remotely, ensuring adherence to safety protocols and responding promptly to any anomalies or emergencies. - Communication: Maintaining clear and continuous communication channels with relevant parties involved in the operation.	Own experience	

7.1.2 Requirements Scenarios-Based

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSB010	Remote Vehicle	Functional	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall be able to send, receive, check and display data from and to the Remote Operator Station	Own experience	

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSBo20	Remote Vehicle	Operational	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall send to Remote Operator Station following data: - Vehicle status (direct vision information): - Speed status - Wheel or steering angle status - Operating mode status (ROL) - Gear selection status - Vehicle status: - AEB status - GPS GNSS RTK Remote Vehicle position and precision - Lights status - Door status - Internal communication enabled status(headphones and/or microphone) - External communication enabled status (headphones and/or microphone) - Horn status - Camera status - Automated Driving System status - Emergency stop status (when triggered) - Network signal strength	Own experience	Table "From Remote Vehicle to Remote Operator Station" in sheet "Definitions"

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSBo30	Remote Vehicle	Operational	ROL2	<p>When in ROL2 mode, the Remote Vehicle shall send to Remote Operator Station following additional data :</p> <ul style="list-style-type: none"> - Driving commands feedback (continuous): - Speed commands feedback - Steering commands feedback - Emergency stop commands feedback - Camera streaming data (continuous): <ul style="list-style-type: none"> - Camera Front - Camera Side - Camera Rear - Camera streaming data (on demand): <ul style="list-style-type: none"> - Camera onboard - Camera external 	Own experience	Table "From Remote Vehicle to Remote Operator Station" in sheet "Definitions"
RSBo40	Remote Vehicle	Operational	ROL3	<p>When in ROL3 mode, the Remote Vehicle shall send to Remote Operator Station following additional data :</p> <ul style="list-style-type: none"> - Driving commands feedback (continuous): - Emergency stop commands feedback - Camera streaming data (continuous): <ul style="list-style-type: none"> - Camera Front - Camera Side - Camera Rear - Camera streaming data (on demand): <ul style="list-style-type: none"> - Camera onboard - Camera external 	Own experience	Table "From Remote Vehicle to Remote Operator Station" in sheet "Definitions"

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSBo50	Remote Vehicle	Operational	ROL4, ROL5	When in ROL4 & ROL5 mode, the Remote Vehicle shall send to Remote Operator Station following additional data : <ul style="list-style-type: none"> - Driving commands feedback (continuous): - Emergency stop commands feedback - Camera streaming data (continuous): - Camera Front - Camera streaming data (on demand): - Camera onboard - Camera external - Camera Side - Camera Rear 	Own experience	Table "From Remote Vehicle to Remote Operator Station" in sheet "Definitions"
RSBo60	Remote Vehicle	Functional	ROL2, ROL3, ROL4, ROL5	The Remote Operator Station shall send, receive, check and execute data from and to the Remote Vehicle	Own experience	
RSBo70	Remote Operator Station	Operational	ROL2, ROL3, ROL4, ROL5	The Remote Operator Station shall send to Remote Vehicle following data: <ul style="list-style-type: none"> - Vehicle commands: - Lights commands - Operating mode commands (ROL) - Doors commands - Internal communication commands (headphones and/or microphone) - External communication commands (headphones and/or microphone) 	Own experience	Table "From Remote Operator Station to Remote Vehicle" in sheet "Definitions"

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
				<ul style="list-style-type: none"> - Horn commands - Camera commands 		
RSBo8o	Remote Operator Station	Operational	ROL2	<p>When in ROL2 mode, the Remote Operator Station shall send to Remote Vehicle following additional data :</p> <ul style="list-style-type: none"> - Driving commands (continuous): - Speed commands - Steering commands - Emergency stop commands - Driving commands (on demand): - Gear commands - Parking brake commands 	Own experience	Table "From Remote Operator Station to Remote Vehicle" in sheet "Definitions"

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSB090	Remote Operator Station	Operational	ROL3	When in ROL3 mode, the Remote Operator Station shall send to Remote Vehicle following additional data : - Driving commands (continuous): - Speed commands - Emergency stop commands - Driving commands (on demand): - Gear commands - Parking brake commands	Own experience	Table "From Remote Operator Station to Remote Vehicle" in sheet "Definitions"
RSB100	Remote Operator Station	Operational	ROL4, ROL5	When in ROL4 & ROL5 mode, the Remote Operator Station shall send to Remote Vehicle following additional data : - Driving commands (continuous): - Emergency stop commands	Own experience	Table "From Remote Operator Station to Remote Vehicle" in sheet "Definitions"
RSB110	Remote Operator Station	Functional	ROL4	The Remote Operator Station shall allow the Remote Operator to define a path for the Remote Vehicle	Own experience	
RSB120	Remote Vehicle	Functional	ROL4	When in ROL4 mode, the Remote Vehicle shall be able to follow a path defined by the Remote Operator while controlling speed automatically	Own experience	
RSB130	Remote Operator Station	Functional	ROL2, ROL3	The Remote Operator Station shall display the vehicle's camera views to show the entire perimeter of the vehicle.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L 221/14 Art. 6.4 ISO 16505:2019

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSB140	Remote Operator Station	Functional	ROL2, ROL3, ROL4, ROL5	The Remote Operator Station shall display the vehicle's camera views to show the entire inside space of the vehicle.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L 221/14 Art. 6.4 ISO 16505:2019
RSB150	Remote Operator Station	Functional	ROL2	The Remote Operator Station shall be equipped with all basic driving equipment.	Own experience	List of basic driving equipment: - Driving wheel - Pedals - Seat - Gear shifter (if applicable) - Dashboard - Shifting gears (if applicable)
RSB160	Remote Operator Station	Functional	ROL2	The Remote Operator Station shall replicate every primary action possible in a standard car.	Own experience	List of primary actions: - Accelerating and decelerating - Steering the vehicle - Activating headlights and high beams - Engaging the parking brake - Operating the hazard lights - Shifting gears (if applicable) - Sounding the horn - Activate turn signals
RSB170	Remote Operator Station	Operational	ROL2, ROL3, ROL4, ROL5	There shall be a defined take over procedure for each different ROL	Own experience	

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSB180	Remote Vehicle	Functional	ROL2	The Remote Vehicle shall be equipped with a system allowing the Remote Operator to communicate with the vehicle's surroundings.	Own experience	
RSB190	Remote Operator Station	Functional	ROL2	The Remote Operator Station shall be equipped with a communication system to interact with the vehicle's surroundings.	Own experience	The communication system must include speakers and a microphone.
RSB200	Remote Vehicle	Functional	ROL2	The Remote Vehicle shall be equipped with cameras with sufficient peripheral vision allowing the Remote Operator to control of the Remote Vehicle.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L 221/14 Art. 6.4 ISO 16505:2019
RSB210	Remote Vehicle	Functional	ROL2	The Remote Vehicle shall indicate whether it is currently in remote operating mode	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L 221/32 Art. 3.5.3.1
RSB220	Remote Vehicle	Functional	ROL2	The Remote Vehicle shall be equipped with a communication system to contact the Remote Operator.	Norm	COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 L 221/14 Art. 6.2 ISO 7010 E004
RSB230	Remote Operator Station	Functional	ROL2	The Remote Operator Station shall display visual indication of different state of telemetry information of the Remote Vehicle	Own experience	List of informations : -Speed -Steering -Brake -Stationary brake -Lights -Vehicle driving mode

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSB240	Remote Operator Station	Functional	ROL2	The Remote Operator Station shall receive visual and audio alerts in the critical cases	Own experience	Critical cases : -Failure alerts -AEB triggered or alerts -Network alerts -Changing vehicle driving mode alerts
RSB250	Remote Vehicle	Functional	ROL2, ROL3	The Remote Operator Station shall be equipped with at least one horn remotely controllable	Norm	OETV Art. 82.1 and Annex 11
RSB260	Remote Operator Station	Design	ROL2, ROL3, ROL4, ROL5	According to UN Regulation No. 121, 5.2.2. : To identify a control, a tell-tale or an indicator not included in Table 1 of ISO 2575:2004, the manufacturer may use a symbol of its own conception. Such symbol may include internationally recognized alphabetic or numeric indications. All symbols used shall follow the design principles laid down in paragraph 4. of ISO 2575:2004.	Norm	UN Regulation No. 121 5.2.2. ISO 2575:2021
RSB270	Remote Operator Station	Performance	ROL2, ROL3, ROL4, ROL5	Movements of objects in front of the camera shall be rendered smooth and fluid. The minimum frame rate of the system (update rate of the image information) shall be at least 30 Hz. At low light conditions or while manoeuvring at low speed, the minimum frame rate of the system (i.e. update rate of the image information) shall be at least 15 Hz.	Norm	UN Regulation No. 46 ISO 16505;2019
RSB280	Remote Operator Station	Operational	ROL2, ROL3, ROL4, ROL5	The Remote Operator Station shall indicate necessary driving information to the Remote Operator through symbols, indicator and tell-tales according to existing standards and regulations	Norm	UN Regulation No. 121 ISO 2575;2021

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
RSB290	Remote Operator Station	Operational	ROL2, ROL3, ROL4, ROL5	According to UN Regulation No. 121, 5.2.2.: To identify a control, a tell-tale or an indicator not included in Table 1 or ISO 2575:2004, the manufacturer may use a symbol of its own conception. Such symbol may include internationally recognized alphabetic or numeric indications. All symbols used shall follow the design principles laid down in paragraph 4. of ISO 2575:2004.	Norm	UN Regulation No. 121 5.2.2.

7.1.3 Cybersecurity Requirements

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0010	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication between the vehicle and the TCC shall be authenticated	Norm	UN ECE R155, Annex 5
CR0020	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The integrity of the communication between the vehicle and the TCC should be ensured	Norm	UN ECE R155, Annex 5 ISA/IEC 62443-3-3 SR.38
CR0030	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall verify the authenticity and integrity of messages it receives	Norm	UN ECE R155, Annex 5
CR0040	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall detect potential denial of service attack	Norm	UN ECE R155, Annex 5

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0050	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall recover from potential denial of service attack	Norm	UN ECE R155, Annex 5
CR0060	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall have the capability to detect unauthorized access	Norm	UN ECE R155, Annex 5
CR0070	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall have the capability to prevent unauthorized access	Norm	UN ECE R155, Annex 5
CR0080	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall possess the capability to authenticate the integrity of messages pertaining to remote operation commands	Norm	UN ECE R155, Annex 5
CR0090	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall logs all relevant information regarding remote operation	Norm	UN ECE R155, Annex 5
CR0100	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall implement an unique identification and authentication methodology to ensure the TCC's identity	Norm	UN ECE R155, Annex 5 ISA/IEC 62443-3-3

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0110	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication channel used for the remote operation shall only be used for remote operations	Norm	UN ECE R155, Annex 5
CR0120	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication between the vehicle and the TCC shall be timestamped	Norm	UN ECE R155, Annex 5
CR0130	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The transmission of PII shall be secured to be aligned with LpD and GDPR	Norm	LpD, GDPR
CR0140	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication channel shall be replicable in case of malfunction of the first one	Own experience	
CR0150	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	A specific and detailed topic-specific information security policy for the TCC shall exist.	Norm	ISO 27001:2022, 5.1
CR0160	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Roles with different responsibilities regarding the TCC (e.g. Administrator, Driver, Hardware Specialist, etc...) shall be defined.	Norm	ISO 27001:2022, 5.2, IKT ID.AM-6, IKT ID.GV-2, IKT DE.DP-1, IKT RS.CO-1 ISA/IEC 62443-3-3

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0170	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Roles with different responsibilities regarding the TCC (e.g. Administrator, Driver, Hardware Specialist, etc...) shall be allocated.	Norm	ISO 27001:2022, 5.2, IKT ID.AM-6, IKT ID.GV-2, IKT DE.DP-1, IKT RS.CO-1 ISA/IEC 62443-3-3
CR0180	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Conflicting duties and responsibilities of people working with TCCs shall be segregated.	Norm	ISO 27001:2022, 5.3, IKT PR.AC-4
CR0190	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Information (strategic, tactical and operational) relating to information security threats to TCCs shall be collected.	Norm	ISO 27001:2022, 5.7, IKT ID.RA-1, IKT ID.RA-2, IKT ID.RA-3
CR0200	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Information (strategic, tactical and operational) relating to information security threats to TCCs shall be analysed.	Norm	ISO 27001:2022, 5.7
CR0210	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	An inventory of information about TCCs shall be maintained.	Norm	ISO 27001:2022, 5.9, IKT ID.AM-2
CR0220	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Rules for the acceptable use of TCCs shall be defined.	Norm	ISO 27001:2022, 5.10

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0230	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Rules for the acceptable use of TCCs shall be known by all relevant people.	Norm	ISO 27001:2022, 5.10
CR0240	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication between the vehicle and the TCC shall be traceable.	Norm	ISO 27001:2022, 5.14
CR0250	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Non-repudiation shall be ensured during communication between vehicle and TCC.	Norm	ISO 27001:2022, 5.14
CR0260	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	A chain-of-custody shall be maintained during communication between vehicle and TCC	Norm	ISO 27001:2022, 5.14
CR0270	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication service shall be reliable according to its needs.	Norm	ISO 27001:2022, 5.14
CR0280	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The communication service shall be available according to its needs.	Norm	ISO 27001:2022, 5.14

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0290	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Malware which can be transmitted during communication shall be detected.	Norm	ISO 27001:2022, 5.14, IKT DE.CM-4
CR0300	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Communicating with a wrong recipient shall be impossible	Norm	ISO 27001:2022, 5.14
CR0310	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Rules to control physical and logical access to the TCC shall be established.	Norm	ISO 27001:2022, 5.15, IKT PR.AC-1
CR0320	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Physical entry controls to rooms with TCCs shall be implemented.	Norm	ISO 27001:2022, 5.15
CR0330	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Logical access controls to TCCs shall be implemented.	Norm	ISO 27001:2022, 5.15
CR0340	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Physical and logical access to TCCs shall be logged.	Norm	ISO 27001:2022, 5.15, 8.15

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0350	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	A specific login-identity shall only be linked to a single person to be able to hold the person accountable for actions performed.	Norm	ISO 27001:2022, 5.16
CR0360	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Login-identities shall be removed immediately if they are no longer used.	Norm	ISO 27001:2022, 5.16
CR0370	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Non-guessable passwords or PINs shall be enforced.	Norm	ISO 27001:2022, 5.17, IKT PR.AC-7
CR0380	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Unique passwords or PINs shall be enforced.	Norm	ISO 27001:2022, 5.17, IKT PR.AC-7
CR0390	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Default authentication information as predefined or provided by vendors shall be changed immediately	Norm	ISO 27001:2022, 5.17
CR0400	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Secret authentication information shall be kept confidential	Norm	ISO 27001:2022, 5.17

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0410	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Strong passwords according to best practice recommendations shall be used	Norm	ISO 27001:2022, 5.17
CR0420	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Strong passwords according to best practice recommendations shall be enforced	Norm	ISO 27001:2022, 5.17, IKT PR.AC-7
CR0430	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Same passwords or PINs shall not be used across distinct services and systems	Norm	ISO 27001:2022, 5.17
CR0440	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Password change at first, initial login shall be enforced	Norm	ISO 27001:2022, 5.17, IKT PR.AC-7
CR0450	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Password changes as necessary (e.g. after an incident) shall be enforced	Norm	ISO 27001:2022, 5.17, IKT PR.AC-8
CR0460	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Re-use of passwords shall be impossible	Norm	ISO 27001:2022, 5.17, IKT PR.AC-9

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0470	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Usage of commonly used passwords shall be impossible	Norm	ISO 27001:2022, 5.17, IKT PR.AC-10
CR0480	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Usage of compromised username-password-combinations from hacked systems shall be impossible	Norm	ISO 27001:2022, 5.17
CR0490	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Passwords or PINs shall not be readable while being entered.	Norm	ISO 27001:2022, 5.17
CR0500	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Passwords or PINs shall be stored in protected form	Norm	ISO 27001:2022, 5.17
CR0510	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Passwords or PINs shall be transmitted in protected form	Norm	ISO 27001:2022, 5.17
CR0520	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Password encryption and hashing shall be performed according to approved cryptographic techniques for passwords.	Norm	ISO 27001:2022, 5.17 ISA/IEC 62443-3-3 SR4.3

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0530	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Access rights for TCCs shall be removed if not used anymore.	Norm	ISO 27001:2022, 5.18, IKT PR.AC-1
CR0540	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Access rights for TCCs shall be given only after authorisation was successful. (Dual Approval)	Norm	ISO 27001:2022, 5.18, IKT PR.AC-1, IKT PR.AC-2 ISA/IEC 62443-3-3
CR0550	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Supplier's products or services shall only be used if they have adequate information security controls in place.	Norm	ISO 27001:2022, 5.19, IKT ID.SC-3
CR0560	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	ICT services suppliers propagating the defined security requirements throughout the supply chain shall be required.	Norm	ISO 27001:2022, 5.19, IKT ID.SC-4
CR0570	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Changes made by supplier shall be monitored.	Norm	ISO 27001:2022, 5.22, 8.16, IKT PR.IP-3, IKT DE.CM-6
CR0580	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	A common method/process for reporting information security events including point of contact shall be established	Norm	ISO 27001:2022, 5.24

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0590	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Only competent people shall be allowed to handle issues related to information security incidents	Norm	ISO 27001:2022, 5.24, IKT PR.IP-9, IKT RS.CO-1
CR0600	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Containing TCCs which are affected from information security incidents shall be possible	Norm	ISO 27001:2022, 5.26, IKT PR.IP-9, IKT RS.MI-1
CR0610	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Evidence shall be collected in case of an incident.	Norm	ISO 27001:2022, 5.26, IKT PR.IP-9
CR0620	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	All involved response activities regarding incidents shall be properly logged for later analysis.	Norm	ISO 27001:2022, 5.26, 8.15, IKT PR.IP-9
CR0630	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Evidence regarding information security events shall be identified.	Norm	ISO 27001:2022, 5.28
CR0640	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Evidence regarding information security events shall be collected.	Norm	ISO 27001:2022, 5.28

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0650	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Evidence regarding information security events shall be preserved.	Norm	ISO 27001:2022, 5.28
CR0660	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Information security shall be maintained during a disruption.	Norm	ISO 27001:2022, 5.29
CR0670	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The business continuity requirements for TCCs shall be determined (e.g. failsafe, load balancing, hot swap)	Norm	ISO 27001:2022, 5.30, IKT ID.BE-5
CR0680	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Business continuity plans for TCCs shall be defined.	Norm	ISO 27001:2022, 5.30, IKT ID.RA-4
CR0690	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Business continuity plans for TCCs shall be tested regularly.	Norm	ISO 27001:2022, 5.30
CR0700	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Records should be protected from loss.	Norm	ISO 27001:2022, 5.33

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0710	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Records should be protected from destruction.	Norm	ISO 27001:2022, 5.33
CR0720	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Records should be protected from falsification.	Norm	ISO 27001:2022, 5.33
CR0730	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Records shall be protected from unauthorized access.	Norm	ISO 27001:2022, 5.33, IKT PR.AC-2
CR0740	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Records shall be protected from unauthorized release.	Norm	ISO 27001:2022, 5.33
CR0750	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be independently reviewed/tested regarding information security.	Norm	ISO 27001:2022, 5.35
CR0760	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Operating procedures shall be properly defined.	Norm	ISO 27001:2022, 5.37

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0770	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Background verification checks on all Drivers shall be conducted prior to gaining access to the TCCs.	Norm	ISO 27001:2022, 6.1, IKT PR.AC-1, IKT PR.AC-6, IKT PR.IP-11
CR0780	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Drivers shall receive appropriate Information security awareness based on education and training.	Norm	ISO 27001:2022, 6.3, IKT PR.AT-1, IKT PR.AT-2, IKT PR.AT-5
CR0790	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Drivers shall ensure appropriate security measures if they can access TCCs from remote or working from remote.	Norm	ISO 27001:2022, 6.7
CR0800	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall include appropriate measures if they can be accessed from remote	Norm	ISO 27001:2022, 6.7, IKT PR.AC-3
CR0810	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs remote access to the system shall be logged.	Norm	ISO 27001:2022, 6.7, 8.15, IKT PR.AC-3
CR0820	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Drivers shall report observed or suspected information security events concerning TCCs.	Norm	ISO 27001:2022, 6.8

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0830	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall report observed or suspected information security events automatically.	Norm	ISO 27001:2022, 6.8
CR0840	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be located in secure areas.	Norm	ISO 27001:2022, 7.1
CR0850	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Rooms with TCCs shall only be accessible after authorisation.	Norm	ISO 27001:2022, 7.2, IKT PR.AC-1, IKT PR.AC-2
CR0860	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Access to rooms with TCCs shall be continuously monitored.	Norm	ISO 27001:2022, 7.2, 8.16, IKT DE.CM-2, IKT DE.CM-7
CR0870	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Video Monitoring shall be in places/rooms for locations where TCCs are installed	Norm	ISO 27001:2022, 7.4, IKT DE.CM-2, IKT DE.CM-7
CR0880	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Rooms with TCCs shall be equipped with an alarm system.	Norm	ISO 27001:2022, 7.4

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0890	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall not be exposed to environmental threats (e.g. heat, humidity, earthquakes, fire, flooding, etc...)	Norm	ISO 27001:2022, 7.5
CR0900	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall not be exposed to physical threats (e.g. hits, theft, vandalism, etc...)	Norm	ISO 27001:2022, 7.5
CR0910	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Rooms with TCCs shall be automatically locked.	Norm	ISO 27001:2022, 7.6
CR0920	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be locked when not in use.	Norm	ISO 27001:2022, 7.7
CR0930	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Screens of TCCs shall not be exposed to shoulder surfing respectively shall not be placed with windows behind the driver's position.	Norm	ISO 27001:2022, 7.8
CR0940	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Connectors for peripherals and removable storage media ports should be appropriately protected or disabled.	Norm	ISO 27001:2022, 7.10, 8.1

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR0950	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Norm	ISO 27001:2022, 7.11
CR0960	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Cables carrying power, data or supporting information services shall be protected from interception.	Norm	ISO 27001:2022, 7.12, IKT PR.DS-2
CR0970	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Cables carrying power, data or supporting information services shall be protected from interference.	Norm	ISO 27001:2022, 7.12, IKT PR.DS-2
CR0980	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Cables carrying power, data or supporting information services shall be protected from damage.	Norm	ISO 27001:2022, 7.12, IKT PR.DS-2
CR0990	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be maintained correctly.	Norm	ISO 27001:2022, 7.13
CR1000	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be included in a monitored maintenance programme	Norm	ISO 27001:2022, 7.13, 8.16, IKT DE.CM-7

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1010	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Maintenance of TCCs shall be logged / recorded, independent whether carried out on-site or remote	Norm	ISO 27001:2022, 7.13, 8.15, IKT PR.MA-1, IKT PR.MA-2
CR1020	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be disposed in a secure way, if they are not needed any-more	Norm	ISO 27001:2022, 7.14
CR1030	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be registered in a central asset register	Norm	ISO 27001:2022, 8.1
CR1040	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall restrict the installation of software	Norm	ISO 27001:2022, 8.1
CR1050	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall receive security updates automatically	Norm	ISO 27001:2022, 8.1
CR1060	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall have access controls in place	Norm	ISO 27001:2022, 8.1

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1070	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Storage devices of TCCs shall be encrypted	Norm	ISO 27001:2022, 8.1
CR1080	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be protected against malware	Norm	ISO 27001:2022, 8.1, 8.7
CR1090	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	It shall be possible to remotely disable, delete or lock out TCCs	Norm	ISO 27001:2022, 8.1
CR1100	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be backed-up regularly.	Norm	ISO 27001:2022, 8.1, 8.13, IKT PR.IP-4
CR1110	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be used only for one purpose, hence e.g. web access shall be disabled	Norm	ISO 27001:2022, 8.1
CR1120	Remote Operator	Cybersecurity	ROL2, ROL3, ROL4, ROL5	User shall log-off once they are not using the TCC anymore	Norm	ISO 27001:2022, 8.1, 8.15

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1130	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall not be used for personal usage	Norm	ISO 27001:2022, 8.1
CR1140	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	If TCCs do not use WiFi, the WiFi shall be disabled by default	Norm	ISO 27001:2022, 8.1
CR1150	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Users with Privileged Access Rights shall be identified	Norm	ISO 27001:2022, 8.2, IKT PR.AC-1, IKT PR.AC-6
CR1160	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Privileged access rights shall be allocated on a event-by-event basis	Norm	ISO 27001:2022, 8.2, IKT PR.AC-1
CR1170	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Remote drivers shall not have privileged access rights for normal day usage	Norm	ISO 27001:2022, 8.2, IKT PR.AC-1, IKT PR.AT-2
CR1180	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	All things carried out with an account having privileged access rights shall be logged for audit purposes	Norm	ISO 27001:2022, 8.2, 8.15

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1190	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Accounts with privileged access rights shall be linked to one person only.	Norm	ISO 27001:2022, 8.2, IKT PR.AC-1, IKT PR.AC-6, IKT PR.AT-2
CR1200	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall not let unauthorized or unknown users have access to sensitive information	Norm	ISO 27001:2022, 8.3, IKT PR.AC-2, IKT PR.AC-4, IKT PR.AC-6
CR1210	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	It shall be possible to control what data is accessible by which user	Norm	ISO 27001:2022, 8.3, IKT PR.DS-1
CR1220	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall incorporate granular control over who can access what information and applications	Norm	ISO 27001:2022, 8.3
CR1230	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Access to source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled.	Norm	ISO 27001:2022, 8.4, IKT PR.AC-1
CR1240	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Secure authentication technologies shall be used	Norm	ISO 27001:2022, 8.5

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1250	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Multi Factor Authentication shall be used	Norm	ISO 27001:2022, 8.5, IKT PR.AC-7 ISA/ IEC 62443-3-3
CR1260	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	All log in attempts shall be logged	Norm	ISO 27001:2022, 8.5, 8.15 ISA/IEC 62443-3-3
CR1270	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Passwords shall not be visible while entering them	Norm	ISO 27001:2022, 8.5, IKT PR.AC-7
CR1280	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall have enough resources to operate securely	Norm	ISO 27001:2022, 8.6, IKT ID.BE-5, IKT PR.DS-4
CR1290	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Vulnerabilities of TCCs shall be reduced actively	Norm	ISO 27001:2022, 8.7, IKT ID.RA-1, IKT PR.IP-12, IKT DE.CM-8, IKT RS.AN-5, IKT RS.MI-3
CR1300	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Malware detection mechanisms shall be updated regularly	Norm	ISO 27001:2022, 8.7

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1310	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Technical vulnerabilities shall be managed actively	Norm	ISO 27001:2022, 8.8, IKT ID.RA-1, IKT PR.IP-12, IKT RS.AN-5, IKT RS.MI-3
CR1320	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Configurations, including security configurations, of TCC-hardware shall be established, documented, implemented, monitored and reviewed.	Norm	ISO 27001:2022, 8.9, 8.16
CR1330	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Configurations, including security configurations, of TCC-software shall be established, documented, implemented, monitored and reviewed.	Norm	ISO 27001:2022, 8.9
CR1340	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Information stored on TCCs shall be deleted if not used anymore	Norm	ISO 27001:2022, 8.10, IKT PR.IP-6
CR1350	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The deletion of Information stored on TCCs shall be documented/logged	Norm	ISO 27001:2022, 8.10
CR1360	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Data Masking shall be implemented where sensitive data is in use	Norm	ISO 27001:2022, 8.11

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1370	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be equipped with appropriate Data Loss Prevention	Norm	ISO 27001:2022, 8.12, IKT PR.DS-5
CR1380	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be set up redundantly to ensure continuous operation	Norm	ISO 27001:2022, 8.14, IKT ID.BE-5
CR1390	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCC' logs shall be analysed in a proper manner	Norm	ISO 27001:2022, 8.15, IKT PR.PT-1
CR1400	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be monitored continuously	Norm	ISO 27001:2022, 8.16, IKT PR.PT-1, IKT DE.CM-7
CR1410	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Networks shall be monitored continuously	Norm	ISO 27001:2022, 8.16, IKT DE.CM-1
CR1420	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Clocks from TCCs and vehicles shall be synchronized	Norm	ISO 27001:2022, 8.17

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1430	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Utility programs used on TCC shall not harm hardware or software	Norm	ISO 27001:2022, 8.18
CR1440	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Installing software on TCCs shall follow secure procedures	Norm	ISO 27001:2022, 8.19
CR1450	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Only specialists shall be allowed to make software changes on TCCs	Norm	ISO 27001:2022, 8.19
CR1460	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Networks and network devices should be secured to protect information in systems and applications.	Norm	ISO 27001:2022, 8.20, IKT PR.PT-4
CR1470	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Networks and network devices should be managed to protect information in systems and applications.	Norm	ISO 27001:2022, 8.20
CR1480	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Networks and network devices should be controlled to protect information in systems and applications.	Norm	ISO 27001:2022, 8.20

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1490	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall only connect to authorized networks	Norm	ISO 27001:2022, 8.21, IKT PR.AC-5 ISA/IEC 62443-3-3
CR1500	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs access to external websites should be managed to reduce exposure to malicious content.	Norm	ISO 27001:2022, 8.23
CR1510	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall follow appropriate rules of cryptography	Norm	ISO 27001:2022, 8.24
CR1520	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Appropriate key management for in TCCs or Communication used keys shall be used at any time	Norm	ISO 27001:2022, 8.24 ISA/IEC 62443-3-3
CR1530	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	If TCCs software or hardware changes, appropriate information security requirements shall be applied	Norm	ISO 27001:2022, 8.26
CR1540	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCC architecture shall include information security principles (e.g. N-1-redundancy, minimal Security configurations)	Norm	ISO 27001:2022, 8.27, IKT PR.IP-1

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1550	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Testing TCCs shall include security testing (e.g. with pentests, vulnerability scans)	Norm	ISO 27001:2022, 8.29, IKT DE.CM-8, IKT RS.AN-5
CR1560	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	If TCCs development is outsourced, the partners shall be directed, monitored and their activities reviewed,	Norm	ISO 27001:2022, 8.30, IKT DE.CM-6
CR1570	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Changes to TCC shall be subject to change management procedures.	Norm	ISO 27001:2022, 8.32, IKT PR.IP-3
CR1580	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be tested in secure environments and setups	Norm	ISO 27001:2022, 8.33
CR1590	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall implement security by design to minimize risks	Norm	UN ECE R155, Annex 5
CR1600	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall have a safe-state in case of losing the communication between the vehicle and the TCC, link FuSa requirements	Norm	UN ECE R156

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1610	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall manage different privilege of authorisation levels	Norm	UN ECE R155, Annex 5
CR1620	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle logs shall be sent to the TCC or cloud environment	Norm	ISA/IEC 62443-3-3 SR3.9 NIST SP800-53 AU-9(2)
CR1630	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall store cryptographic keys in a secure manner (e.g HSM)	Norm	UN ECE R155, Annex 5
CR1640	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall have a secure boot mechanism to avoid any firmware modification	Studies	security risk assessment
CR1650	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall have a anti-rollback mechanism to avoid a software rollback with vulnerability	Studies	security risk assessment
CR1660	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Unnecessary Ports of the computer managing the remote operation shall be physically hardened if not removed	Studies	security risk assessment

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1670	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	A security assessment shall be performed to assess risks regarding system interconnections	Norm	NIST SP800-53
CR1680	Communication	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The software update shall be download through a secure communication	Norm	UN ECE R156
CR1690	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The software update shall be installed when the vehicle is in a safe & secure state	Norm	UN ECE R156
CR1700	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The network shall be segmented between critical systems(controls systems) and less critical system (infotainment)	Norm	NIST SP800-53 ISA/IEC 62443-3-3 SR5.1
CR1710	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall have the capability to react to unauthorized access	Norm	UN ECE R155, Annex 5
CR1720	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCC server shall only be accessible from recognized computer	Norm	ISA/IEC 62443-3-3 -SR2.3

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
CR1730	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCC's network shall be segmented to ensure an isolation of the TCC from non-critical systems	Norm	ISA/IEC 62443-3-3 SR5.X
CR1740	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	Norm	ISA/IEC 62443-3-3 SR6.2
CR1750	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Sensors' data integrity shall be ensured inside the Remote Vehicle	Norm	UN ECE R155, Annex 5
CR1760	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Sensors' data integrity shall be ensured during the transfer between the Remote Vehicle and the TCC	Norm	UN ECE R155, Annex 5
CR1770	Remote Vehicle	Cybersecurity	ROL2, ROL3, ROL4, ROL5	The Remote Vehicle shall implement the least privilege concept between critical and less critical component inside the vehicle	Norm	NIST SP800-53
CR1780	Remote Vehicle	Cybersecurity	ROL2, ROL3,	The Remote Vehicle shall send redundancy sensors information to the TCC	Studies	security risk assessment

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
			ROL4, ROL5			
CR1790	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Cyber risks concerning TCCs shall be addressed in the organization wide risk management	Norm	IKT ID.GV-4, IKT ID.RM-2
CR1800	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Integrity of Firmware, OS, Software, Hardware and Data shall be verified continually	Norm	IKT PR.DS-1, IKT PR.DS-2, IKT PR.DS-6, IKT PR.DS-8
CR1810	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Suppliers providing parts of TCCs shall be monitored and audited regularly	Norm	ISO 5.21, IKT ID.SC-4, IKT DE.CM-6
CR1820	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Lifecycle management shall be applied for TCCs, Hardware and software and TCCs, hardware and software out where the end of support is reached shall not be used anymore	Norm	IKT PR.IP-2
CR1830	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Back-Up tests shall be conducted regularly	Norm	IKT PR.IP-4
CR1840	Remote Operator Station	Cybersecurity	ROL2, ROL3,	Incident recovery shall be tested regularly	Norm	IKT PR.IP-9

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
			ROL4, ROL5			
CR1850	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	TCCs shall be designed and configured in a way, that a minimal level of functionality is guaranteed at all time needed.	Norm	IKT PR.PT-3
CR1860	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Thresholds for alerts regarding information security incidents occurring at TCCs shall be defined	Norm	IKT DE.AE-5, IKT RS.CO-2
CR1870	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Information on cyber security incidents shall be aggregated form different sources (Not only TCC)	Norm	IKT DE.AE-3, IKT DE.AE-5
CR1880	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Malware detection mechanisms shall be implemented	Norm	ISO 8.7, IKT DE.CM-4
CR1890	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Monitoring of TCCs and networks shall be tested regularly	Norm	IKT DE.DP-3
CR1900	Remote Operator Station	Cybersecurity	ROL2, ROL3,	Incident response plans shall be executed promptly and properly during or after the detection of an incident	Norm	ISO 27001:2022 5.26, IKT RS.RP-1

ID	Category	Req. Type	ROL	Requirement Description	Source	Source Spec
			ROL4, ROL5			
CR1910	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Incident response plans shall exist and be updated regularly	Norm	ISO 27001:2022 5.26, IKT RS.RP-1, IKT RS.AN-4, IKT RS.IM-2
CR1920	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Security incidents at TCCs shall be kept to a minimum	Norm	IKT RS.MI-2
CR1930	Remote Operator Station	Cybersecurity	ROL2, ROL3, ROL4, ROL5	Incident recovery plans shall exist and be updated regularly	Norm	IKT RC.IM-2

7.2 A2 - Levels of Driving Automation According to ISO/SAE PAS 22736:2021

The classification system proposed in standard ISO/SAE PAS 22736 [69], the internationally recognized Taxonomy for driving automation systems, comprises six levels of driving automation, from conventional driving with no automation (Level 0) to full automation (Level 5).

This standard formalizes the Taxonomy previously defined in SAE J3016 within the ISO framework, making it authoritative global reference. While the descriptions of the levels remain consistent with SAE J3016, ISO/SAE PAS 22736 does not include the graphical representation of the automation levels that is familiar from earlier SAE J3016 publications which are presented in the figure below.

	SAE LEVEL 0	SAE LEVEL 1	SAE LEVEL 2	SAE LEVEL 3	SAE LEVEL 4	SAE LEVEL 5
What does the human in the driver's seat have to do?	You <u>are</u> driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You <u>are not</u> driving when these automated driving features are engaged – even if you are seated in “the driver’s seat”		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			These are automated driving features		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/acceleration support to the driver	These features provide steering AND brake/acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met	This feature can drive the vehicle under all conditions	
Example Features	<ul style="list-style-type: none"> • automatic emergency braking • blind spot warning • lane departure warning 	<ul style="list-style-type: none"> • lane centering OR • adaptive cruise control 	<ul style="list-style-type: none"> • lane centering AND • adaptive cruise control at the same time 	<ul style="list-style-type: none"> • traffic jam chauffeur 	<ul style="list-style-type: none"> • local driverless taxi • pedals/steering wheel may or may not be installed 	<ul style="list-style-type: none"> • same as level 4, but feature can drive everywhere in all conditions

Source: [93]

The six levels are defined as follows (“.” verbatim from SAE J3016 standard):

- **Level 0: No Driving Automation:**
 - „The performance by the driver of the entire dynamic driving task (DDT), even when enhanced by active safety systems “.
 - Driver performs DDT, object and event detection and response (OEDR) and DDT fallback.
 - No defined operational design domain (ODD).

- **Level 1: Driver Assistance:**
 - „The sustained and ODD-specific execution by a driving automation system of either the lateral or the longitudinal vehicle motion control subtask of the DDT (but not both simultaneously) with the expectation that the driver performs the remainder of the DDT “.
 - DDT performed by driver and system, OEDR and fallback by Driver.
 - Limited ODD.
- **Level 2: Partial Driving Automation:**
 - The performance by the driver of the entire DDT, even when enhanced by active safety systems. “
 - DDT fully done by system, driver performs OEDR and fallback.
 - Limited ODD.
- **Level 3: Conditional Driving Automation:**
 - „The sustained and ODD-specific execution by a driving automation system of both the lateral and longitudinal vehicle motion control subtasks of the DDT with the expectation that the driver completes the OEDR subtask and supervises the driving automation system. “
 - System performs DDT and OEDR. Fallback-ready user is available to become the driver in case of fallback.
 - Limited ODD.
- **Level 4: High Driving Automation:**
 - „The sustained and ODD-specific performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will need to intervene. “
 - DDT, OEDR and DDT fallback fully controlled by system.
 - Limited ODD.
- **Level 5: Full Driving Automation:**
 - „The sustained and unconditional (i.e., not ODD-specific) performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will need to intervene. “
 - DDT, OEDR and DDT fallback fully controlled by system.
 - Unlimited ODD.

7.3 A3 - Taxonomy of Remote Operation Levels (ROL)

Remote Operation Level	ROL 1	ROL 2	ROL 3	ROL 4	ROL 5
Designation	Remote Controller Driving	Tele Driving	Teleassistance Operation L1	Teleassistance Operation L2	Monitoring
Task	Full control of the vehicle Act like a normal driver Communication	Full control on the vehicle Act like a normal driver Communication	Path drawing Speed control Lights or other control Communication	Path drawing Path confirmation Communication	Supervision Communication
DDT responsibility of operator	Full	Full	Speed application	None	None
OEDR responsibility of operator	Full	None	None	None	None
Remote driver support system active	Collision Avoidance System AEBS*	Collision Avoidance System AEBS*	Vehicle fully automated	Vehicle fully automated	Vehicle fully automated
Responsibility	On-site Operator	Remote Operator	Automated Vehicle	Automated Vehicle	Automated Vehicle
Operator location	< 6 m	On the territory	On the territory	On the territory	On the territory
Speed limitation	6 km/h	6 km/h	Road limitation	Road limitation	Road limitation
Operational safety criteria (MRM trigger)	Remote controller communication	Video latency Driving data command latency	ADS operational Internet connection	ADS operational Internet connection	ADS operational Internet connection
Typical situation	Tele Driving not possible - Bad Internet connection - Bad visibility through camera	Teleassistance L1 not possible - ADS not able to drive autonomously - Complex manoeuvre (e.g. put vehicle at the side of the road)	Teleassistance L2 not possible - Vehicle stationary for too long - Improve traffic flow - Priority agreement situation	Vehicle need confirmation or new path - System limitation - Obstruction on the driving path - Vehicle uncertainty - Complex situation	- Automated Vehicle in normal operation - Part of troubleshooting procedure



*AEBS = Advanced Emergency Braking System
*OEDR = Object and Event Detection and Response

7.4 A4 – Details Cybersecurity Test Results

The following tables summarise all the cybersecurity requirements and indicate whether they were addressed (80 out of 193) during the cybersecurity testing validation phase or not (see 7.1 for the complete list of requirements and 4.7 for the description of the cybersecurity tests).

7.4.1 Remote Operator Station

Cybersecurity test results for Remote Operator Station			
ID	Category	Description	Validated (Yes/No)
CR016	Remote Operator Station	A specific and detailed topic-specific information security policy for the TCC shall exist.	No
CR017	Remote Operator Station	Roles with different responsibilities regarding the TCC (e.g. Administrator, Driver, Hardware Specialist, etc...) shall be defined.	Yes
CR018	Remote Operator Station	Roles with different responsibilities regarding the TCC (e.g. Administrator, Driver, Hardware Specialist, etc...) shall be allocated.	No
CR019	Remote Operator Station	Conflicting duties and responsibilities of people working with TCCs shall be segregated.	No
CR020	Remote Operator Station	Information (strategic, tactical and operational) relating to information security threats to TCCs shall be collected.	No
CR021	Remote Operator Station	Information (strategic, tactical and operational) relating to information security threats to TCCs shall be analysed.	No
CR022	Remote Operator Station	An inventory of information about TCCs shall be maintained.	Yes
CR023	Remote Operator Station	Rules for the acceptable use of TCCs shall be defined.	No
CR024	Remote Operator Station	Rules for the acceptable use of TCCs shall be known by all relevant people.	No
CR032	Remote Operator Station	Rules to control physical and logical access to the TCC shall be established.	Yes
CR033	Remote Operator Station	Physical entry controls to rooms with TCCs shall be implemented.	Yes
CR034	Remote Operator Station	Logical access controls to TCCs shall be implemented.	Yes
CR035	Remote Operator Station	Physical and logical access to TCCs shall be logged.	Yes
CR036	Remote Operator Station	A specific login-identity shall only be linked to a single person to be able to hold the person accountable for actions performed.	Yes
CR037	Remote Operator Station	Login-identities shall be removed immediately if they are not longer used.	No
CR038	Remote Operator Station	Non-guessable passwords or PINs shall be enforced.	Yes
CR039	Remote Operator Station	Unique passwords or PINs shall be enforced.	Yes

ID	Category	Description	Validated (Yes/No)
CR040	Remote Operator Station	Default authentication information as predefined or provided by vendors shall be changed immediately	No
CR043	Remote Operator Station	Strong passwords according to best practice recommendations shall be enforced	Yes
CR045	Remote Operator Station	Password change at first, initial login shall be enforced	No
CR046	Remote Operator Station	Password changes as necessary (e.g. after an incident) shall be enforced	No
CR047	Remote Operator Station	Re-use of passwords shall be impossible	No
CR048	Remote Operator Station	Usage of commonly-used passwords shall be impossible	No
CR049	Remote Operator Station	Usage of compromised username-password-combinations from hacked systems shall be impossible	No
CR050	Remote Operator Station	Passwords or PINs shall not be readable while being entered.	No
CR051	Remote Operator Station	Passwords or PINs shall be stored in protected form	No
CR052	Remote Operator Station	Passwords or PINs shall be transmitted in protected form	No
CR053	Remote Operator Station	Password encryption and hashing shall be performed according to approved cryptographic techniques for passwords.	Yes
CR054	Remote Operator Station	Access rights for TCCs shall be removed if not used anymore.	No
CR055	Remote Operator Station	Access rights for TCCs shall be given only after authorisation was successful. (Dual Approval)	No
CR056	Remote Operator Station	Supplier's products or services shall only be used if they have adequate information security controls in place.	No
CR057	Remote Operator Station	ICT services suppliers propagating the defined security requirements throughout the supply chain shall be required.	No
CR058	Remote Operator Station	Changes made by supplier shall be monitored.	No
CR059	Remote Operator Station	A common method/process for reporting information security events including point of contact shall be established	No
CR060	Remote Operator Station	Only competent people shall be allowed to handle issues related to information security incidents	No
CR061	Remote Operator Station	Containing TCCs which are affected from information security incidents shall be possible	No
CR062	Remote Operator Station	Evidence shall be collected in case of an incident.	No
CR063	Remote Operator Station	All involved response activities regarding incidents shall be properly logged for later analysis.	No
CR064	Remote Operator Station	Evidence regarding information security events shall be identified.	No
CR065	Remote Operator Station	Evidence regarding information security events shall be collected.	No
CR066	Remote Operator Station	Evidence regarding information security events shall be preserved.	No

ID	Category	Description	Validated (Yes/No)
CR067	Remote Operator Station	Information security shall be maintained during a disruption.	No
CR068	Remote Operator Station	The business continuity requirements for TCCs shall be determined (e.g. failsafe, load balancing, hot swap)	No
CR069	Remote Operator Station	Business continuity plans for TCCs shall be defined.	No
CR070	Remote Operator Station	Business continuity plans for TCCs shall be tested regularly.	No
CR071	Remote Operator Station	Records should be protected from loss.	No
CR072	Remote Operator Station	Records should be protected from destruction.	No
CR073	Remote Operator Station	Records should be protected from falsification.	No
CR074	Remote Operator Station	Records shall be protected from unauthorized access.	No
CR075	Remote Operator Station	Records shall be protected from unauthorized release.	No
CR076	Remote Operator Station	TCCs shall be independently reviewed/tested regarding information security.	Yes
CR077	Remote Operator Station	Operating procedures shall be properly defined.	No
CR081	Remote Operator Station	TCCs shall include appropriate measures if they can accessed from remote	Yes
CR082	Remote Operator Station	TCCs remote access to the system shall be logged.	No
CR084	Remote Operator Station	TCCs shall report observed or suspected information security events automatically.	No
CR085	Remote Operator Station	TCCs shall be located in secure areas.	Yes
CR086	Remote Operator Station	Rooms with TCCs shall only be accessible after authorisation.	Yes
CR087	Remote Operator Station	Access to rooms with TCCs shall be continuously monitored.	Yes
CR088	Remote Operator Station	Video Monitoring shall be in places/rooms for locations where TCCs are installed	Yes
CR089	Remote Operator Station	Rooms with TCCs shall be equipped with an alarm system.	Yes
CR090	Remote Operator Station	TCCs shall not be exposed to environmental threats (e.g. heat, humidity, earthquakes, fire, flooding, etc...)	Yes
CR091	Remote Operator Station	TCCs shall not be exposed to physical threats (e.g. hits, theft, vandalism, etc...)	Yes
CR092	Remote Operator Station	Rooms with TCCs shall be automatically locked.	Yes
CR093	Remote Operator Station	TCCs shall be locked when not in use.	Yes
CR094	Remote Operator Station	Screens of TCCs shall not be exposed to shoulder surfing respectively shall not be placed with windows behind the drivers position.	Yes

ID	Category	Description	Validated (Yes/No)
CR095	Remote Operator Station	Connectors for peripherals and removable storage media ports should be appropriately protected or disabled.	No
CR096	Remote Operator Station	TCCs shall be protected from power failures and other disruptions caused by failures in supporting utilities.	No
CR097	Remote Operator Station	Cables carrying power, data or supporting information services shall be protected from interception.	No
CR098	Remote Operator Station	Cables carrying power, data or supporting information services shall be protected from interference.	No
CR099	Remote Operator Station	Cables carrying power, data or supporting information services shall be protected from damage.	No
CR100	Remote Operator Station	TCCs shall be maintained correctly.	No
CR101	Remote Operator Station	TCCs shall be included in a monitored maintenance programme	No
CR102	Remote Operator Station	Maintenance of TCCs shall be logged / recorded, independent whether carried out on-site or remote	No
CR103	Remote Operator Station	TCCs shall be disposed in a secure way, if they are not needed anymore	No
CR104	Remote Operator Station	TCCs shall be registered in a central asset register	No
CR105	Remote Operator Station	TCCs shall restrict the installation of software	Yes
CR106	Remote Operator Station	TCCs shall receive security updates automatically	Yes
CR107	Remote Operator Station	TCCs shall have access controls in place	Yes
CR108	Remote Operator Station	Storage devices of TCCs shall be encrypted	Yes
CR109	Remote Operator Station	TCCs shall be protected against malware	Yes
CR110	Remote Operator Station	It shall be possible to remotely disable, delete or lock out TCCs	Yes
CR111	Remote Operator Station	TCCs shall be backed-up regularly.	Yes
CR112	Remote Operator Station	TCCs shall be used only for one purpose, hence e.g. web access shall be disabled	Yes
CR114	Remote Operator Station	TCCs shall not be used for personal usage	No
CR115	Remote Operator Station	If TCCs do not use WiFi, the WiFi shall be disabled by default	Yes
CR116	Remote Operator Station	Users with Privileged Access Rights shall be identified	Yes
CR117	Remote Operator Station	Privileged access rights shall be allocated on a event-by-event basis	Yes
CR118	Remote Operator Station	Remote drivers shall not have privileged access rights for normal day usage	Yes

ID	Category	Description	Validated (Yes/No)
CR119	Remote Operator Station	All things carried out with an account having privileged access rights shall be logged for audit purposes	Yes
CR120	Remote Operator Station	Accounts with privileged access rights shall be linked to one person only.	Yes
CR121	Remote Operator Station	TCCs shall not let unauthorized or unknown users have access to sensitive information	Yes
CR122	Remote Operator Station	It shall be possible to control what data is accessible by which user	No
CR123	Remote Operator Station	TCCs shall incorporate granular control over who can access what information and applications	Yes
CR124	Remote Operator Station	Access to source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled.	Yes
CR125	Remote Operator Station	Secure authentication technologies shall be used	Yes
CR126	Remote Operator Station	Multi Factor Authentication shall be used	Yes
CR127	Remote Operator Station	All log in attempts shall be logged	Yes
CR128	Remote Operator Station	Passwords shall not be visible while entering them	Yes
CR129	Remote Operator Station	TCCs shall have enough resources to operate securely	No
CR130	Remote Operator Station	Vulnerabilities of TCCs shall be reduced actively	Yes
CR131	Remote Operator Station	Malware detection mechanisms shall be updated regularly	Yes
CR132	Remote Operator Station	Technical vulnerabilities shall be managed actively	Yes
CR133	Remote Operator Station	Configurations, including security configurations, of TCC-hardware shall be established, documented, implemented, monitored and reviewed.	Yes
CR134	Remote Operator Station	Configurations, including security configurations, of TCC-software shall be established, documented, implemented, monitored and reviewed.	Yes
CR135	Remote Operator Station	Information stored on TCCs shall be deleted if not used anymore	Yes
CR136	Remote Operator Station	The deletion of Information stored on TCCs shall be documented/logged	No
CR137	Remote Operator Station	Data Masking shall be implemented where sensitive data is in use	No
CR138	Remote Operator Station	TCCs shall be equipped with appropriate Data Loss Prevention	Yes
CR139	Remote Operator Station	TCCs shall be set up redundantly to ensure continuous operation	No
CR140	Remote Operator Station	TCC' logs shall be analysed in a proper manner	No
CR141	Remote Operator Station	TCCs shall be monitored continuously	Yes
CR142	Remote Operator Station	Networks shall be monitored continuously	Yes

ID	Category	Description	Validated (Yes/No)
CR143	Remote Operator Station	Clocks from TCCs and vehicles shall be synchronized	No
CR144	Remote Operator Station	Utility programs used on TCC shall not harm hardware or software	No
CR145	Remote Operator Station	Installing software on TCCs shall follow secure procedures	No
CR146	Remote Operator Station	Only specialists shall be allowed to make software changes on TCCs	Yes
CR147	Remote Operator Station	Networks and network devices should be secured to protect information in systems and applications.	Yes
CR148	Remote Operator Station	Networks and network devices should be managed to protect information in systems and applications.	Yes
CR149	Remote Operator Station	Networks and network devices should be controlled to protect information in systems and applications.	Yes
CR150	Remote Operator Station	TCCs shall only connect to authorized networks	Yes
CR151	Remote Operator Station	TCCs access to external websites should be managed to reduce exposure to malicious content.	Yes
CR152	Remote Operator Station	TCCs shall follow appropriate rules of cryptography	Yes
CR153	Remote Operator Station	Appropriate key management for in TCCs or Communication used keys shall be used at any time	Yes
CR154	Remote Operator Station	If TCCs software or hardware changes, appropriate information security requirements shall be applied	No
CR155	Remote Operator Station	TCC architecture shall include information security principles (e.g. N-1-redundancy, minimal Security configurations)	No
CR156	Remote Operator Station	Testing TCCs shall include security testing (e.g. with pentests, vulnerability scans)	Yes
CR157	Remote Operator Station	If TCCs development is outsourced, the partners shall be directed, monitored and their activities reviewed,	No
CR158	Remote Operator Station	Changes to TCC shall be subject to change management procedures.	No
CR159	Remote Operator Station	TCCs shall be tested in secure environments and setups	Yes
CR173	Remote Operator Station	TCC server shall only be accessible from recognized computer	Yes
CR174	Remote Operator Station	TCC's network shall be segmented to ensure an isolation of the TCC from non-critical systems	Yes
CR180	Remote Operator Station	Cyber risks concerning TCCs shall be addressed in the organization wide risk management	No
CR181	Remote Operator Station	Integrity of Firmware, OS, Software, Hardware and Data shall be verified continually	No
CR182	Remote Operator Station	Suppliers providing parts of TCCs shall be monitored and audited regularly	No
CR183	Remote Operator Station	Lifecycle management shall be applied for TCCs, Hardware and software and TCCs, hardware and software out where the end of support is reached shall not be used anymore	No

ID	Category	Description	Validated (Yes/No)
CR184	Remote Operator Station	Back-Up tests shall be conducted regularly	No
CR185	Remote Operator Station	Incident recovery shall be tested regularly	No
CR186	Remote Operator Station	TCCs shall be designed and configured in a way, that a minimal level of functionality is guaranteed at all times needed.	No
CR187	Remote Operator Station	Thresholds for alerts regarding information security incidents occurring at TCCs shall be defined	No
CR188	Remote Operator Station	Information on cyber security incidents shall be aggregated from different sources (Not only TCC)	No
CR189	Remote Operator Station	Malware detection mechanisms shall be implemented	No
CR190	Remote Operator Station	Monitoring of TCCs and networks shall be tested regularly	No
CR191	Remote Operator Station	Incident response plans shall be executed promptly and properly during or after the detection of an incident	No
CR192	Remote Operator Station	Incident response plans shall exist and be updated regularly	No
CR193	Remote Operator Station	Security incidents at TCCs shall be kept to a minimum	No
CR194	Remote Operator Station	Incident recovery plans shall exist and be updated regularly	No

7.4.2 Remote Vehicle

Cybersecurity test results for Remote Vehicle			
ID	Category	Description	Validated (Yes/No)
CR004	Remote Vehicle	The Remote Vehicle shall verify the authenticity and integrity of messages it receives	No
CR005	Remote Vehicle	The Remote Vehicle shall detect potential denial of service attack	No
CR006	Remote Vehicle	The Remote Vehicle shall recover from potential denial of service attack	No
CR007	Remote Vehicle	The Remote Vehicle shall have the capability to detect unauthorized access	No
CR008	Remote Vehicle	The Remote Vehicle shall have the capability to prevent unauthorized access	Yes
CR009	Remote Vehicle	The Remote Vehicle shall possess the capability to authenticate the integrity of messages pertaining to remote operation commands	No
CR010	Remote Vehicle	The Remote Vehicle shall logs all relevant information regarding remote operation	No
CR011	Remote Vehicle	The Remote Vehicle shall implement a unique identification and authentication methodology to ensure the TCC's identity	Yes
CR012	Remote Vehicle	The communication channel used for the remote operation shall only be used for remote operations	Yes
CR160	Remote Vehicle	The Remote Vehicle shall implement security by design to minimize risks	No
CR161	Remote Vehicle	The Remote Vehicle shall have a safe-state in case of losing the communication between the vehicle and the TCC, link FuSa requirements	No
CR162	Remote Vehicle	The Remote Vehicle shall manage different privilege of authorisation levels	Yes
CR163	Remote Vehicle	The Remote Vehicle logs shall be sent to the TCC or cloud environment	No
CR164	Remote Vehicle	The Remote Vehicle shall store cryptographic keys in a secure manner (e.g. HSM)	No
CR165	Remote Vehicle	The Remote Vehicle shall have a secure boot mechanism to avoid any firmware modification	Yes
CR166	Remote Vehicle	The Remote Vehicle shall have an anti-rollback mechanism to avoid a software rollback with vulnerability	No
CR167	Remote Vehicle	Unnecessary Ports of the computer managing the remote operation shall be physically hardened if not removed	No
CR168	Remote Vehicle	A security assessment shall be performed to assess risks regarding system interconnections	Yes
CR169	Communication	The software update shall be download through a secure communication	No
CR170	Remote Vehicle	The software update shall be installed when the vehicle is in a safe & secure state	No
CR171	Remote Vehicle	The network shall be segmented between critical systems (controls systems) and less critical system (infotainment)	Yes

CR172	Remote Vehicle	The Remote Vehicle shall have the capability to react to unauthorized access	Yes
CR175	Remote Vehicle	The Remote Vehicle shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	No
CR176	Remote Vehicle	Sensors' data integrity shall be ensured inside the Remote Vehicle	No
CR177	Remote Vehicle	Sensors' data integrity shall be ensured during the transfer between the Remote Vehicle and the TCC	No
CR178	Remote Vehicle	The Remote Vehicle shall implement the least privilege concept between critical and less critical component inside the vehicle	Yes
CR179	Remote Vehicle	The Remote Vehicle shall send redundancy sensors information to the TCC	No

7.4.3 Communication

Cybersecurity test results for Communications

ID	Category	Description	Validated (Yes/No)
CR001	Communication	The communication between the vehicle and the TCC shall be authenticated	Yes
CR002	Communication	The integrity of the communication between the vehicle and the TCC should be ensured	No
CR013	Communication	The communication between the vehicle and the TCC shall be timestamped	No
CR014	Communication	The transmission of PII shall be secured to be aligned with LpD and GDPR	No
CR015	Communication	The communication channel shall be replicable in case of failure of the first one	No
CR025	Communication	The communication between the vehicle and the TCC shall be traceable.	No
CR026	Communication	Non-repudiation shall be ensured during communication between vehicle and TCC.	Yes
CR027	Communication	A chain-of-custody shall be maintained during communication between vehicle and TCC	No
CR028	Communication	The communication service shall be reliable according to its needs.	No
CR029	Communication	The communication service shall be available according to its needs.	Yes
CR030	Communication	Malware which can be transmitted during communication shall be detected.	No
CR031	Communication	Communicating with a wrong recipient shall be impossible	Yes

7.4.4 Remote Operator

Cybersecurity test results for Remote Operator			
ID	Category	Description	Validated (Yes/No)
CR041	Remote Operator	Secret authentication information shall be kept confidential	No
CR042	Remote Operator	Strong passwords according to best practice recommendations shall be used	Yes
CR044	Remote Operator	Same passwords or PINs shall not be used across distinct services and systems	No
CR078	Remote Operator	Background verification checks on all Drivers shall be conducted prior to gaining access to the TCCs.	No
CR079	Remote Operator	Drivers shall receive appropriate Information security awareness based on education and training.	No
CR080	Remote Operator	Drivers shall ensure appropriate security measures if they can access TCCs from remote or working from remote.	No
CR083	Remote Operator	Drivers shall report observed or suspected information security events concerning TCCs.	No
CR113	Remote Operator	User shall log-off once they are not using the TCC anymore	Yes

7.5 A5 - Survey Results from LOXO Operators

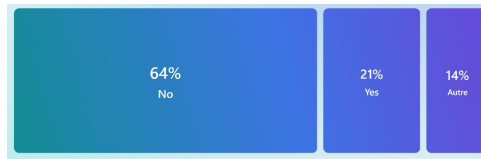
The numbers shown in the blue boxes between 1 – Insufficient and 4 – Very Good (e.g., 3.3 for the first question) represent the average ratings given by respondents to the survey. The percentages listed below the ratings (for example, 0%, 14%, 35%, and 50% for the first question) represent the percentage of people who rated 1, 2, 3, or 4. In summary, the average rating for the first question is 3.3, indicating that the remote operation is more than well-designed, with half of the respondents rating the centre as very well-designed (4).

Questions	Answers
Is the Remote Operation clearly designed?	<div style="text-align: center; background-color: #e1f5fe; padding: 10px;"> <p style="font-size: 24px; margin: 0;">3.3</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;">1 0 %</div> <div style="text-align: center;">2 14 %</div> <div style="text-align: center;">3 35 %</div> <div style="text-align: center;">4 50 %</div> </div> </div>
Is the positioning of the screens and the tablet (for telemetry feedback) intuitive?	<div style="text-align: center; background-color: #e1f5fe; padding: 10px;"> <p style="font-size: 24px; margin: 0;">3.3</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;">1 0 %</div> <div style="text-align: center;">2 0 %</div> <div style="text-align: center;">3 64 %</div> <div style="text-align: center;">4 35 %</div> </div> </div>
Are the screens big enough?	<div style="text-align: center; background-color: #e1f5fe; padding: 10px;"> <p style="font-size: 24px; margin: 0;">3.8</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;">1 0 %</div> <div style="text-align: center;">2 0 %</div> <div style="text-align: center;">3 14 %</div> <div style="text-align: center;">4 85 %</div> </div> </div>
Are the display and use of the tablet (e.g. for orders allocation) intuitive?	<div style="text-align: center; background-color: #e1f5fe; padding: 10px;"> <p style="font-size: 24px; margin: 0;">3.2</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;">1 0 %</div> <div style="text-align: center;">2 21 %</div> <div style="text-align: center;">3 28 %</div> <div style="text-align: center;">4 50 %</div> </div> </div>
How would you rate the ease of use of the remote operation system?	<div style="text-align: center; background-color: #e1f5fe; padding: 10px;"> <p style="font-size: 24px; margin: 0;">4.0</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;">1 0 %</div> <div style="text-align: center;">2 0 %</div> <div style="text-align: center;">3 21 %</div> <div style="text-align: center;">4 50 %</div> <div style="text-align: center;">5 28 %</div> </div> </div>
	Comfortable

<p>What are your impressions of the driving kit (steering wheel and pedal)?</p>	<p>Steering wheel good, pedals a bit cheap without good feedback on how much one is accelerating</p> <hr/> <p>It's nice except the reverse gear of the gear box</p> <hr/> <p>It feels a bit light compared to real pedals and steering wheel</p> <hr/> <p>It would be nice to add some text explaining what each steering wheel button does (instead of logos)</p> <hr/> <p>It was a very nice experience and very impressive</p> <hr/> <p>Functional and easy to use</p>
<p>How do you feel about the arrangement of the TCC – Teleoperation Control Centre (seat, steering wheel, pedals, screens)?</p>	<p>The seats are comfortable, the steering wheel has a direct response, I have the same screen at home, it's very good, the pedals are ok</p> <hr/> <p>I feel good in the operation Perfect Comfy</p> <hr/> <p>Seat is too low, not adequate for tall persons, pedals too close to seat and steering wheel too close to knees</p> <hr/> <p>Tablet interface can be improved</p> <hr/> <p>The driving kit is good, but the low driving position could be improved</p> <hr/> <p>It was good. But the quality of the video screens wasn't very good</p>
<p>Is the allocation of buttons on the steering wheel clear and intuitive?</p>	<div style="background-color: #e0f2f7; padding: 10px; text-align: center;"> <h1 style="margin: 0;">3.2</h1> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;"> 1 0 % </div> <div style="text-align: center;"> 2 14 % </div> <div style="text-align: center;"> 3 42 % </div> <div style="text-align: center;"> 4 42 % </div> </div> </div>
<p>Is the transition from teleoperation to automated mode intuitive?</p>	<div style="background-color: #e0f2f7; padding: 10px; text-align: center;"> <h1 style="margin: 0;">3.5</h1> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;"> 1 0 % </div> <div style="text-align: center;"> 2 7 % </div> <div style="text-align: center;"> 3 35 % </div> <div style="text-align: center;"> 4 57 % </div> </div> </div>
<p>Is the transition from automated to teleoperation mode intuitive?</p>	<div style="background-color: #e0f2f7; padding: 10px; text-align: center;"> <h1 style="margin: 0;">3.5</h1> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;"> 1 0 % </div> <div style="text-align: center;"> 2 7 % </div> <div style="text-align: center;"> 3 28 % </div> <div style="text-align: center;"> 4 64 % </div> </div> </div>

<p>Are the camera views of the vehicle adequate?</p>	<table border="1"> <tr><th>Rating</th><th>Percentage</th></tr> <tr><td>1</td><td>0 %</td></tr> <tr><td>2</td><td>21 %</td></tr> <tr><td>3</td><td>35 %</td></tr> <tr><td>4</td><td>42 %</td></tr> </table>	Rating	Percentage	1	0 %	2	21 %	3	35 %	4	42 %
Rating	Percentage										
1	0 %										
2	21 %										
3	35 %										
4	42 %										
<p>Is the Augmented Reality (e.g. red guiding lines) effective and helping?</p>	<table border="1"> <tr><th>Rating</th><th>Percentage</th></tr> <tr><td>1</td><td>0 %</td></tr> <tr><td>2</td><td>14 %</td></tr> <tr><td>3</td><td>71 %</td></tr> <tr><td>4</td><td>14 %</td></tr> </table>	Rating	Percentage	1	0 %	2	14 %	3	71 %	4	14 %
Rating	Percentage										
1	0 %										
2	14 %										
3	71 %										
4	14 %										
<p>Which elements could be included or modified to better the teleoperation?</p>	<p>Nothing</p> <hr/> <p>Quality of the Cameras</p> <hr/> <p>Personalized configurations for each teleoperator (e.g. button allocations, rear mirror flipped, etc...)</p> <hr/> <p>Having sound all the time</p> <hr/> <p>Less buttons on the wheel, more features on the tablet</p> <hr/> <p>Noise cancelling (headphones)</p> <hr/> <p>Augmented reality from LiDAR data to improve the confidence feeling</p> <hr/> <p>Walls around the remote operation centre</p>										
<p>How did the system identify you as a certified teleoperator?</p>	<p>Receive of login on Teleop App</p>										
<p>What was the log-in-mechanism into the Remote Operation Centre?</p>	<p>Username and password</p>										
<p>Did you have to use a multi-factor authentication?</p>	<table border="1"> <tr><th>Response</th><th>Percentage</th></tr> <tr><td>No</td><td>85 %</td></tr> <tr><td>Yes</td><td>14 %</td></tr> </table>	Response	Percentage	No	85 %	Yes	14 %				
Response	Percentage										
No	85 %										
Yes	14 %										
<p>How aware of any incident response plan, in case of a cybersecurity breach or safety incident?</p>	<table border="1"> <tr><th>Rating</th><th>Percentage</th></tr> <tr><td>1</td><td>7 %</td></tr> <tr><td>2</td><td>21 %</td></tr> <tr><td>3</td><td>42 %</td></tr> <tr><td>4</td><td>28 %</td></tr> </table>	Rating	Percentage	1	7 %	2	21 %	3	42 %	4	28 %
Rating	Percentage										
1	7 %										
2	21 %										
3	42 %										
4	28 %										
<p>Are the emergency and shutdown procedures clearly described and easily accessible?</p>	<table border="1"> <tr><th>Rating</th><th>Percentage</th></tr> <tr><td>1</td><td>0 %</td></tr> <tr><td>2</td><td>21 %</td></tr> <tr><td>3</td><td>21 %</td></tr> <tr><td>4</td><td>57 %</td></tr> </table>	Rating	Percentage	1	0 %	2	21 %	3	21 %	4	57 %
Rating	Percentage										
1	0 %										
2	21 %										
3	21 %										
4	57 %										

Did you receive cybersecurity training material (e.g. awareness of potential cyber threats and how to respond) during your training for teleoperating vehicles?



Should the TCC – Teleoperation Control Centre integrate additional information to enhance teleoperation safety and security?



What are the things that distract you most when you're teleoperating the vehicle?

People come ask you randomly questions while driving or phone calls

Camera quality
Quality of the video

To be honest, it didn't distract me at all. I noticed everything

Other people in the room
People talking around me when remote driving

Watching to click the correct button

Nothing, a panel similar to those in a bus "Do not talk to the driver" is used

Shifter isn't necessary

It doesn't need to be improved, I was happy with it

Better camera quality

Better camera resolution, less lag, options to flip rear camera to mirror, automatic deactivation of side indicators after turning, better sound feedback from ODD through micros on the vehicle, bigger tablet with bigger buttons and mor intuitive front end

What components, elements, functionalities or options (HW, SW, display, etc.) could be added or removed to improve the experience or make it clearer?

Sound, Display the automated path that will be taken on the screen, highlight obstacles

Auto launch of the TCC app, more fluid tablet, app for the tablet, better (pro) UI design, better steering/gear hardware

A better seat & something more intuitive on the tablet

One more screen for LiDAR view, better augmented reality, on big display instead of four

Better augmented reality, ambient sound always active

Some issues could be fixed faster

Everything has been improved in the best possible way

What is not being done well at the moment and what could be improved?

LiDAR sensor are too sensible

Most important would be camera resolution and seat position

Platform dynamics

Camera latency and freeze



bibliography

- [1] SAAM, “SAAM - Swiss Association for Autonomous Mobility,” 2025, 13 01. [Online]. Available: <https://www.saam.swiss/>. [Accessed 21 01 2025].
- [2] SwissMoves, “SwissMoves,” 2018. [Online]. Available: <https://swissmoves.ch>. [Accessed 09 12 2024].
- [3] ASTRA, “Vernehmlassung: Verordnung über das automatisierte Fahren,” 18 10 2023. [Online]. Available: <https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet/rechtliche-situation/vernehmlassung-verordnung-automatisiertes-fahren.html>.
- [4] admin.ch, “Bundesrat ermöglicht automatisiertes Fahren,” 13 12 2024. [Online]. Available: <https://www.astra.admin.ch/astra/de/home/dokumentation/medienmitteilungen/anzeige-meldungen.msg-id-103529.html>. [Accessed 17 12 2024].
- [5] ASTRA/OFROU/FEDRO, “Ordonnance sur la conduite automatisée (OCA) - Verordnung über das automatisierte Fahren (VAF),” 13 12 2024. [Online]. Available: <https://www.fedlex.admin.ch/eli/oc/2025/50/de>. [Accessed 25 01 2025].
- [6] M.-A. Fénart, R. Scherwey and G. Python, “Switzerland's first teleoperated vehicle,” ResearchGate, 09 2021. [Online]. Available: https://www.researchgate.net/publication/354472087_Switzerland's_first_teleoperated_vehicle. [Accessed 21 01 2025].
- [7] R. Scherwey, “NRP Project Teleoperation,” 2021. [Online]. Available: https://www.heia-fr.ch/en/applied-research/institutes/isis/research-projects/nrp-p_chs-ccma/. [Accessed 11 12 2024].
- [8] United Nations, “Convention on Road Traffic,” 1949. [Online]. Available: <https://www.worlddriversassociation.com/pdf/CONVENTION%20ON%20ROAD%20TRAFFIC1949.pdf>. [Accessed 21 01 2025].
- [9] Nations, United, “Vienna Convention on the Law of Treaties,” 1969. [Online]. Available: https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf. [Accessed 09 12 2024].
- [10] UNECE, “UN Regulation No. 155 - Cyber security and cyber security management system,” 2021. [Online]. Available: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>. [Accessed 09 12 2024].
- [11] UNECE, “UN Regulation No. 156 - Software update and software update management system,” 2021. [Online]. Available: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update>. [Accessed 09 12 2024].
- [12] R. Scherwey, “Development and implementation of basic infrastructures and technical processes necessary for the approval of automated vehicles according to an adapted legal framework,” 2020. [Online]. Available: https://www.heia-fr.ch/de/anwendungsorientierte-forschung/institute/isis/forschungsprojekte/nrp-p_chs-ccma/. [Accessed 11 12 2024].

- [13] R. Scherwey, “Evaluation and development of the concept of a Swiss Certification Centre and a national Competence Centre for Autonomous Mobility,” 2019. [Online]. Available: https://www.heia-fr.ch/de/anwendungsorientierte-forschung/institute/isis/forschungsprojekte/nrp-e_chs-ccma/. [Accessed 12 9 2022].
- [14] PostAuto, “SmartShuttle,” 13 03 2024. [Online]. Available: <https://swissaam.ch/projects/smartshuttle>. [Accessed 11 12 2024].
- [15] TPF, “Line 100 of TPF,” SAAM, 13 03 2024. [Online]. Available: <https://swissaam.ch/projects/line-100/>. [Accessed 21 01 2025].
- [16] TPG, “AVENUE EU Project,” SAAM, 13 03 2024. [Online]. Available: <https://swissaam.ch/projects/avenue-eu-project/>. [Accessed 21 01 2025].
- [17] MyShuttle, “MyShuttle Zug,” SAAM, 03 13 2024. [Online]. Available: <https://swissaam.ch/projects/my-shuttle/>. [Accessed 21 01 2025].
- [18] BERNMOBIL, “Line 23 of BERNMOBIL (Automated Shuttle),” SAAM, 13 03 2024. [Online]. Available: <https://swissaam.ch/projects/line-23-automated-shuttle/>. [Accessed 21 01 2025].
- [19] SAAM, “Machbarkeitsstudie für die Integration von automatisiertem Ridepooling in Zug,” 13 01 2025. [Online]. Available: <https://www.saam.swiss/de/projekte/feasibility-study-for-automated-ridepooling-integration-in-zug/>. [Accessed 21 01 2025].
- [20] Swiss Transit Lab, “Line 13 of the Swiss Transit Lab,” SAAM, 13 03 2024. [Online]. Available: <https://swissaam.ch/projects/line-13-of-the-swiss-transit-lab/>. [Accessed 21 01 2025].
- [21] PostAuto, “Der Gepäckroboter «Robi» begleitet die Gäste in der Sommersaison,” postauto, 09 06 2022. [Online]. Available: <https://www.postauto.ch/de/ueber-uns-und-aktuelles/aktuelles/2022/der-gepaekroboter-robi-begleitet-die-gaeste-in-der-sommersaison>. [Accessed 21 01 2025].
- [22] PostAuto, “Swiss Post delivery robots in use by Jelmoli,” PostAuto, 29 08 2017. [Online]. Available: <https://www.post.ch/en/about-us/news/2017/swiss-post-delivery-robots-in-use-by-jelmoli>. [Accessed 11 12 2024].
- [23] SwissMoves, “LOXO - Autonomous Goods Delivery Vehicle,” 09 2021. [Online]. Available: <https://swissmoves.ch/index.php/component/content/article/loxo?catid=15&Itemid=123>. [Accessed 09 12 2024].
- [24] “Ko-Pilotprojekt «Planzer – Dynamic Micro-Hub w LOXO»,” Planzer, 19 09 2024. [Online]. Available: <https://planzer-paket.ch/ch/gschichte/ko-pilotprojekt-planzer-dynamic-micro-hub-w-loxo/>. [Accessed 21 01 2025].
- [25] “Builtec Sarl - La technologie d’automatisation (AutoSnow),” *ECHO (No. 3 2024)*, p. 17, 06 2024.
- [26] R. Scherwey and R. Mosqueron, “TaaS - Transport as a Service for Smart Business Parks,” Innosquare, 2023. [Online]. Available: <https://www.innosquare.com/de/projekten/axe-smart-territory/taas/>. [Accessed 09 12 2024].
- [27] R. Scherwey, R. Mosqueron, M.-A. Féart and G. Python, “Mobilité dans les parcs d’affaires intelligents,” *Electrosuisse*, 04 04 2024. [Online]. Available: <https://www.bulletin.ch/fr/news-detail/mobilite-dans-les-parcs-d-affaires-intelligents.html>. [Accessed 09 12 2024].

- [28] LOXO, “LOXO - Digital Driver,” 03 12 2024. [Online]. Available: <https://www.loxo.ch/en/>. [Accessed 21 01 2025].
- [29] A. Autonomy, “Applied Autonomy,” 01 09 2024. [Online]. Available: <https://www.appliedautonomy.no/portfolio>. [Accessed 21 01 2025].
- [30] MIRA, “Gemeinsam die Zukunft der Mobilität gestalten,” MIRA, 01 04 2022. [Online]. Available: <https://www.mira-mobility.com/>. [Accessed 21 01 2025].
- [31] Mobileye, “Mobileye beginnt mit dem Test autonomer Fahrzeuge in Deutschland,” emobilitaetblog, 23 12 2023. [Online]. Available: <https://emobilitaetblog.de/mobileye-beginnt-mit-dem-test-autonomer-fahrzeuge-in-deutschland>. [Accessed 21 01 2025].
- [32] nordicplus, “The first autonomous large bus in the world in open traffic,” 08 09 2022. [Online]. Available: <https://itsnordicplus.com/news/the-first-autonomous-large-bus-in-the-world-in-open-traffic>. [Accessed 21 01 2025].
- [33] Fractional CISO, “The Groundbreaking 2015 Jeep Hack Changed Automotive Cybersecurity,” 21 02 2021. [Online]. Available: <https://fractionalciso.com/the-groundbreaking-2015-jeep-hack-changed-automotive-cybersecurity>. [Accessed 19 09 2022].
- [34] FONES, “Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs,” 5 2021. [Online]. Available: https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/oeffentlicher_verkehr.html. [Accessed 14 9 2022].
- [35] Reuters, “Truly autonomous cars may be impossible without helpful human touch,” 19 09 2022. [Online]. Available: <https://www.reuters.com/technology/truly-autonomous-cars-may-be-impossible-without-helpful-human-touch-2022-09-12>. [Accessed 22 01 2025].
- [36] SwissMoves, “Système d'automatisation et de téléopération pour robots porte-outils agricoles,” 10 2024. [Online]. Available: <https://swissmoves.ch/index.php/component/content/article/autoscale?catid=15&Itemid=123>. [Accessed 09 12 2024].
- [37] EasyMile, “EasyMile First Authorized at Level 4 of Autonomous Driving on Public Roads,” 21 11 2021. [Online]. Available: <https://easymile.com/news/easymile-first-authorized-level-4-autonomous-driving-public-roads>. [Accessed 21 01 2025].
- [38] J. L. Felix Tener, “Driving from a Distance: Challenges and Guidelines for Autonomous Vehicle Teleoperation Interfaces,” 04 2022. [Online]. Available: https://www.researchgate.net/publication/360263621_Driving_from_a_Distance_Challenges_and_Guidelines_for_Autonomous_Vehicle_Teleoperation_Interfaces. [Accessed 21 01 2025].
- [39] H. H. Gaetano Graf, “User Requirements for Remote Teleoperation-based Interfaces,” 09 2020. [Online]. Available: https://www.researchgate.net/publication/347579148_User_Requirements_for_Remote_Teleoperation-based_Interfaces. [Accessed 21 01 2025].
- [40] J. Y. C. Chen, E. . C. Haas and M. Barnes, “Human Performance Issues and User Interface Design for Teleoperated Robots,” 12 2007. [Online]. Available: https://www.researchgate.net/publication/3421856_Human_Performance_Issues_and_User_Interface_Design_for_Teleoperated_Robots. [Accessed 21 01 2025].

- [41] DriveU.auto, “DriveU.auto Releases Teleoperation Taxonomy,” 20 06 2023. [Online]. Available: <https://driveu.auto/press-release/driveu-auto-releases-teleoperation-taxonomy/>. [Accessed 21 01 2025].
- [42] D. L. Zhang, “The Cruise Safety Report: Advancing our safety mission through a transparent and holistic approach,” 2022. [Online]. Available: <https://www.getcruise.com/news/blog/2022/the-cruise-safety-report-advancing-our-safety-mission-through-a-transparent-and-holistic-approach/>. [Accessed 21 01 2025].
- [43] Soliton Systems K.K., Yusa, Yoh, “Draft: Regulations for the latency time of communication at the remote,” 04 2022. [Online]. Available: https://www.soliton.co.jp/lp/rp/img/2030720-20220401Er06Fr09_En.pdf. [Accessed 21 01 2025].
- [44] A. S. H. A. a. M. O. Carmen Kettwich, “A Helping Human Hand: Relevant Scenarios for the Remote Operation of Highly Automated Vehicles in Public Transport,” 35 04 2022. [Online]. Available: https://www.researchgate.net/publication/360176223_A_Helping_Human_Hand_Relevant_Scenarios_for_the_Remote_Operation_of_Highly_Automated_Vehicles_in_Public_Transport. [Accessed 21 01 2025].
- [45] migros, “Der erste selbstfahrende Lieferdienst der Schweiz beginnt seine Testphase,” 08 02 2023. [Online]. Available: <https://corporate.migros.ch/de/news/migronomous>. [Accessed 21 12 2024].
- [46] Swisscom, “Swisscom helps Holcim and Volvo to test the quarry of the future,” 23 05 2022. [Online]. Available: <https://www.swisscom.ch/en/about/news/2022/05/23-autonome-dumper-im-steinbruch.html>. [Accessed 21 12 2024].
- [47] UNECE, “World Forum for Harmonization of Vehicle Regulations (WP.29),” 03 2022. [Online]. Available: <https://unece.org/transport/vehicle-regulations/world-forum-harmonization-vehicle-regulations-wp29>. [Accessed 09 12 2024].
- [48] U. GRVA, “Working Party on Automated/Autonomous and Connected Vehicles - Introduction,” 2024. [Online]. Available: <https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction>. [Accessed 21 01 2025].
- [49] UNECE, “UN Regulation No. 79 Revision 5,” 2024. [Online]. Available: <https://unece.org/transport/documents/2023/10/working-documents/un-regulation-no-79-revision-5>. [Accessed 09 12 2024].
- [50] UNECE, “UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS),” 2021. [Online]. Available: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks>. [Accessed 09 12 2024].
- [51] International Organization for Standardization ISO, “ISO 23793 series Intelligent transport systems – Minimal risk manoeuvre (MRM) for automated driving,” 2024. [Online]. Available: <https://www.iso.org/standard/81711.html>. [Accessed 21 01 2025].
- [52] International Organization for Standardization ISO, “ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering,” 2021. [Online]. Available: <https://www.iso.org/standard/70918.html>. [Accessed 09 12 2024].
- [53] ISO/TC, “ISO/TC 22 Road Vehicles,” 1947. [Online]. Available: <https://www.iso.org/committee/46706.html>. [Accessed 21 01 2025].

- [54] République Française, “Décret n° 2021-873 du 29 juin 2021,” 2021. [Online]. Available: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043729532>. [Accessed 21 01 2025].
- [55] République Française, “Ordonnance n° 2021-443 du 14 avril 2021,” 2021. [Online]. Available: https://www.ecologie.gouv.fr/sites/default/files/documents/Ordonnance%20article%2031%20of%20Mobility%20Law_0.pdf. [Accessed 21 01 2025].
- [56] KBA, “Legislation on Autonomous Driving,” 2022. [Online]. Available: https://www.kba.de/EN/Themen_en/Marktueberwachung_en/Produktpruefungen_en/AutomatisiertesAutonomesFahren_en/Gesetzgebung_en/gesetzgebung_autonomes_fahren_node_en.html. [Accessed 21 01 2025].
- [57] ASTRA FB 1681, “Auswirkungen des automatisierten Fahrens; Teilprojekt 1: Nutzungsszenarien und Auswirkungen,” 2020. [Online]. Available: <https://www.mobilityplatform.ch/de/research-data-shop/product/1681>. [Accessed 21 01 2025].
- [58] ASTRA FB 1684, “Auswirkungen des automatisierten Fahrens; Teilprojekt 5: Mischverkehr,” 2020. [Online]. Available: <https://www.mobilityplatform.ch/de/research-data-shop/product/1684>. [Accessed 21 01 2025].
- [59] ASTRA FB 1694, “Auswirkungen des automatisierten Fahrens; Teilprojekt 3: Umgang mit Daten,” 2020. [Online]. Available: <https://www.mobilityplatform.ch/de/research-data-shop/product/1694>. [Accessed 21 01 2025].
- [60] Lawcom, “Remote driving,” 09 03 2023. [Online]. Available: <https://lawcom.gov.uk/project/remote-driving/>. [Accessed 21 01 2025].
- [61] ENISA, “European Union Agency for Cybersecurity,” 11 2019. [Online]. Available: <https://www.enisa.europa.eu/publications/smart-cars>. [Accessed 09 12 2024].
- [62] International Organization for Standardization ISO, “ISO 26262-x series, Road vehicles - Functional safety,” 2018. [Online]. Available: <https://www.iso.org>.
- [63] International Organization for Standardization ISO, “ISO 21448 Safety of the Intended Functionality (SOTIF),” 2022. [Online]. Available: <https://www.iso.org/standard/77490.html>. [Accessed 21 01 2025].
- [64] International Organization for Standardization ISO, “ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements,” 2022. [Online]. Available: <https://www.iso.org/standard/27001>. [Accessed 21 01 2025].
- [65] International Organization for Standardization ISO, “ISO/TS 23792 series Motorway Chauffeur Systems (MCS),” 2023. [Online]. Available: <https://www.iso.org/standard/76964.html>. [Accessed 21 01 2025].
- [66] International Organization for Standardization ISO, “ISO/DIS 7856 Remote Support for Low-Speed AV Systems - Performance Requirements, System Requirements and Performance Test Procedures,” 2024. [Online]. Available: <https://www.iso.org/standard/82951.html>. [Accessed 21 01 2025].
- [67] International Organization for Standardization ISO, “Report on standardisation prospective for automated vehicles (RoSPAV),” 01 2021. [Online]. Available: <https://www.iso.org/committee/46706.html>. [Accessed 09 12 2024].

- [68] BMDV- Bundesministerium für Digitales und Verkehr, “Autonomes Fahren im öffentlichen Verkehr - Ein Handbuch mit Vorschlägen für die Umsetzung in der kommunalen Praxis,” 27 11 2024. [Online]. Available: https://fops.de/wp-content/uploads/2024/11/BMDV_Handbuch_Autonomes_Fahren_Im_Oeffentlichen_Verkehr.pdf. [Accessed 16 12 2024].
- [69] ISO/SAE PAS 22736, “Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles,” 2021. [Online]. Available: <https://www.iso.org/standard/73766.html>. [Accessed 21 01 2025].
- [70] T-Systems, “IAA Mobility,” 2021. [Online]. Available: https://exhibitors.iaa.de/download/1126_9_62_1838_62_1_104/iaa_teleoperation-brueckentechnologie-fuer-ad.pdf.
- [71] ISO 34501:2022, *Road vehicles – Test scenarios for automated driving systems – Vocabulary*, Geneva, Switzerland: International Organization for Standardization, 2022.
- [72] S. Neumeier, P. Wintersberger, A.-K. Frison, A. Becher, C. Facchi and A. Riener, “Teleoperation: The Holy Grail to Solve Problems of Automated Driving? Sure, but Latency Matters,” 09 2019. [Online]. Available: https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters. [Accessed 21 01 2025].
- [73] X. Shen, Z. J. Chong, S. Pendleton, G. M. James Fu, B. Qin, E. Frazzoli and M. H. Ang, “Teleoperation of on-road vehicles via immersive telepresence using off-the-shelf components,” in *Intelligent Autonomous Systems 13: Proceedings of the 13th International Conference IAS-13*, 2016.
- [74] J. Davis, C. Smyth and K. McDowell, “The effects of time lag on driving performance and a possible mitigation,” *IEEE Transactions on Robotics*, vol. 26, p. 590–593, 2010.
- [75] Lockheed Martin, “The Cyber Kill Chain,” 25 09 2024. [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. [Accessed 21 01 2025].
- [76] “MITRE | ATT&CK,” 2024. [Online]. Available: <https://attack.mitre.org>. [Accessed 21 01 2025].
- [77] “OWASP - Open Worldwide Application Security Project,” 2024. [Online]. Available: <https://owasp.org/>. [Accessed 21 01 2025].
- [78] ISA, “International Society of Automation,” 09 2024. [Online]. Available: <https://www.isa.org/>. [Accessed 09 12 2024].
- [79] “metasploit - The world’s most used penetration testing framework,” 01 11 2024. [Online]. Available: <https://www.metasploit.com>. [Accessed 21 01 2025].
- [80] BASt - Bundesamt für Strassenwesen, “Technical report of the working group - Research Needs in Teleoperation,” 06 2024. [Online]. Available: <https://www.bast.de/DE/Publikationen/Fachveroeffentlichungen/Fahrzeugtechnik/Downloads-Links/TO-en.html>. [Accessed 09 12 2024].
- [81] S. Neumeier, E. A. Walelgne, V. Bajpaj, J. Ott and C. Facchi, “Measuring the Feasibility of Teleoperated Driving in Mobile Networks,” in *2019 Network Traffic Measurement and Analysis Conference (TMA)*, 2019.

- [82] S. Neumeier, V. Bajpai, M. Neumeier, C. Facchi and J. Ott, “Data Rate Reduction for Video Streams in Teleoperated Driving,” pp. 1-16, 2022.
- [83] A. Hosseini, F. Richthammer and M. Lienkamp, “Predictive Haptic Feedback for Safe Lateral Control of Teleoperated Road Vehicles in Urban Areas,” in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016.
- [84] C. Ju and H. I. Son, “Evaluation of Haptic Feedback in the Performance of a Teleoperated Un- manned Ground Vehicle in an Obstacle Avoidance Scenario,” p. 13, 2019.
- [85] S. Neumeier, S. Stapf and C. Facchi, “The Visual Quality of Teleoperated Driving Scenarios How good is good enough?,” in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2022.
- [86] ASTRA FB 1691, “Auswirkungen des automatisierten Fahrens; Erkenntnisse und Massnahmen aus Sicht des ASTRA,” 10 2020. [Online]. Available: https://www.mobilityplatform.ch/fileadmin/mobilityplatform/normenpool/21781_1691_Inhalt.pdf. [Accessed 09 12 2024].
- [87] J.-M. Georg, J. Feiler, S. Hoffmann and F. Diermeyer, “Sensor and Actuator Latency during Teleoperation of Automated Vehicles,” in *2020 IEEE Intelligent Vehicles Symposium (IV)*, 2020.
- [88] J. Lanir, “Driving from a Distance: Challenges and Guidelines for Autonomous Vehicle Teleoperation Interfaces,” 01 04 2022. [Online]. Available: https://www.researchgate.net/profile/Joel-Lanir/publication/360263621_Driving_from_a_Distance_Challenges_and_Guidelines_for_Autonomous_Vehicle_Teleoperation_Interfaces. [Accessed 21 01 2025].
- [89] S. Hoffmann, F. Willert, M. Hofbauer, A. Schimpe and F. Diermeyer, “Quantifying the Influence of Image Quality on Operator Reaction Times for Teleoperated Road Vehicles,” in *AHFE (2022) International Conference*, 2022.
- [90] M. Oehl, “Linkedin - Visit DLR Braunschweig by HEIA-FR/HEG-FR (SwissMoves) and LOXO,” 01 02 2024. [Online]. Available: https://www.linkedin.com/posts/michael-oehl-10023662_dlr-braunschweig-remote-activity-7158897185437204480-h1ni/. [Accessed 09 12 2024].
- [91] “Regulation No 46 of the Economic Commission for Europe of the United Nations (UNECE) — Uniform provisions concerning the approval of devices for indirect vision and of motor vehicles with regard to the installation of these devices,” 08 08 2024. [Online]. Available: <http://data.europa.eu/eli/reg/2014/46/oj>. [Accessed 21 01 2025].
- [92] “Road vehicles — Ergonomic and performance aspects of Camera Monitor Systems — Requirements and test procedures,” 2019. [Online]. Available: <https://www.iso.org/standard/72000.html>. [Accessed 21 01 2025].
- [93] J. Shuttleworth, “SAE Standards News: J3016 automated-driving graphic update,” 07 01 2019. [Online]. Available: <https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic>. [Accessed 21 01 2025].

Project Conclusion



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

FORSCHUNG IM STRASSENWESEN DES UVEK

Version vom 09.10.2013

Formular Nr. 3: Projektabschluss

erstellt / geändert am: 18.12.2024

Grunddaten

Projekt-Nr.: MB4_20_02E_01

Projekttitel: Minimum requirements for an authorisation to remotely drive automated vehicles in Switzerland

Enddatum: 28.02.2025

Texte

Zusammenfassung der Projektergebnisse:

Das Forschungsprojekt zur Fernsteuerung automatisierter Fahrzeuge (AVs) hat grundlegende Anforderungen für Systeme für den Fernbetrieb (Remote Operation) von führerlosen Fahrzeugen definiert und validiert, um hohe Sicherheits- und Zuverlässigkeitsstandards zu gewährleisten. Eine umfassende Taxonomie für Fernbedienstufen (Remote Operation Levels) wurde entwickelt (ROL1–ROL5), die die Aufgaben und Verantwortlichkeiten von Operatoren klar definiert und Szenarien aus der realen Welt berücksichtigt.

Im Rahmen des Projekts wurden 247 Mindestanforderungen in den Bereichen technische Anforderungen, Cybersicherheit und betriebliche Prozesse identifiziert und in On-Site Tests (Slalom, Parking und weitere Szenarien) definiert. Zu den wichtigsten Ergebnissen gehören:

- **Latenztoleranz:** Keine signifikanten Auswirkungen auf die Manövrierfähigkeit bei Latenzen bis zu 850 ms (bei ROL2 und Geschwindigkeiten des AV bis 6 km/h).
- **Szenariorelevanz:** Szenarien wie "False Positive" Hinderniserkennung bestätigten die Praktikabilität der entwickelten Anforderungen.
- **Cybersicherheit:** 193 spezifische Anforderungen wurden definiert, wovon 80 in Penetrationstests getestet wurden.

Diese Ergebnisse bieten eine robuste Grundlage für die Integration von Systemen für den Fernbetrieb von AVs (Remote Operation System) in die öffentliche Verkehrsinfrastruktur der Schweiz und tragen zur Weiterentwicklung technologischer und regulatorischer Rahmenbedingungen bei.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

Zielerreichung:

Das Projekt verfolgte zwei Hauptziele, die erfolgreich erreicht wurden:

1. **Definition von Mindestanforderungen:**
Die Anforderungen umfassen technische, betriebliche und cybersicherheitsrelevante Aspekte. Eine besondere Stärke des Projekts liegt in der Verbindung internationaler Standards (z. B. UNECE und ISO) mit praxisorientierten Szenarien. Die entwickelten Anforderungen bilden eine Grundlage für die rechtliche Zulassung von Remote Operation Systems.
2. **Erweiterung des Wissens zu Systemen für den Fernbetrieb (Remote Operation Systems):**
Durch die Validierung der Anforderungen in experimentellen Tests und theoretischen Analysen wurden die Grenzen und Einsatzmöglichkeiten solcher Systeme besser verstanden. Ein Beispiel ist die experimentelle Validierung des Szenarios "False Positive"-Hinderniserkennung, das die Relevanz der Anforderungen bekräftigte.

Folgerungen und Empfehlungen:

Das Forschungsprojekt hat wichtige Grundlagen für die sichere und zuverlässige Integration von Systemen für den Fernbetrieb von AVs in die Schweizer Verkehrsinfrastruktur geschaffen. Um den Fortschritt in diesem Bereich nachhaltig zu fördern, sind gezielte Massnahmen und ein Regulierungs- und Steuerungssystem erforderlich. Diese Empfehlungen bieten eine Orientierung für die nächste Phase der Entwicklung und Implementierung.

- **Regulierungs- / Steuerungssystem einführen:**
Es wird empfohlen, ein Regulierungs- und Steuerungssystem zu etablieren, das die Umsetzung der Anforderungen, regelmässige Updates und die Integration neuer Technologien sicherstellt. Das Konsortium könnte hier als unabhängige Instanz fungieren, um den Prozess gemäss der OCA/AFV-Verordnung zu unterstützen.
- **Sicherheitsprinzipien priorisieren:**
Stabile Kommunikationskanäle, redundante Systeme und klare Schulungsstandards sind essenziell, um die Sicherheit von AVs und anderen Verkehrsteilnehmern zu gewährleisten.
- **Weiterentwicklung von Szenarien und Standards:**
Neue Szenarien sollten entwickelt werden, um komplexe städtische Umgebungen, höhere Geschwindigkeiten und widrige Wetterbedingungen zu berücksichtigen. Parallel dazu ist die Harmonisierung nationaler Anforderungen mit internationalen Standards notwendig.

Publikationen:

Keine

Der Projektleiter/die Projektleiterin:

Name: Scherwey Vorname: Roland

Amt, Firma, Institut: HEIA-FR (ROSAS Center), SwissMoves

Unterschrift des Projektleiters/der Projektleiterin:



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

FORSCHUNG IM STRASSENWESEN DES UVEK

Formular Nr. 3: Projektabschluss

Beurteilung der Begleitkommission:

Beurteilung:

Das Projekt hat eine umfassende und systematische Analyse durchgeführt, um die Mindestanforderungen für das ferngesteuerte Fahren automatisierter Fahrzeuge in der Schweiz zu definieren. Besonders hervorzuheben ist die Entwicklung eines Taxonomiesystems für Fernbedienungsstufen (Remote Operation Levels, ROL1–ROL5), das die unterschiedlichen Anforderungen und Verantwortlichkeiten der Operatoren (ROL2-ROL5) für Teleoperation und Teleassistenz und Fahrzeugführer für die manuelle Bedienung (ROL1) präzise abbildet. Die gewählten Validierungsmethoden, wie die szenariobasierte Prüfung und experimentelle Tests (z. B. Slalom- und Parktests), haben die Praxistauglichkeit der Anforderungen untermauert. Die Berücksichtigung spezifischer Szenarien, wie Netzwerkunterbrechungen oder Wetterbedingungen, stellt sicher, dass die Systeme auch in herausfordernden Situationen sicher und zuverlässig funktionieren. Die Cybersecurity-Anforderungen wurden umfassend definiert und es wurden praxisnahe Tests durchgeführt, womit die Resilienz der Systeme gegenüber internen und externen Bedrohungen aufgezeigt werden konnte.

Umsetzung:

Die entwickelte Methodik und die Anforderungen bieten eine solide Grundlage für die praktische Anwendung mittels Testszenarien, experimentellen Tests sowie Cybersecurity-Tests. Die Validierungsergebnisse zeigen, dass die Systeme bei niedrigen Geschwindigkeiten (bis 6 km/h, ROL2) stabil und präzise betrieben werden können, selbst bei erhöhten Netzwerklatenzen (bis zu 850 ms). Die Ergebnisse der Tests zu Szenarien wie "False Positive" Hinderniserkennung und komplexen Manövern wie Einparken zeigen, dass die Anforderungen realistisch und umsetzbar sind. Das Projekt hat auch gezeigt, dass die Anforderungen gut mit internationalen Standards harmonisieren und somit sowohl nationale als auch internationale Integration unterstützen können. Für die breite Anwendung ist jedoch eine sorgfältige Schulung der Operatoren und eine kontinuierliche Weiterentwicklung der Systemtechnologie notwendig. Die Ergebnisse legen nahe, dass die entwickelten Anforderungen unmittelbar in die Praxis überführt werden können, um Pilotprojekte oder die Einführung in reguläre Anwendungen zu unterstützen.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

weitergehender Forschungsbedarf:

Für die sichere Integration von Systemen für den Fernbetrieb von AVs (Remote Operation Systems) bleibt weiterer Forschungsbedarf in zentralen Bereichen. Insbesondere sind vertiefte Analysen zur Optimierung der Netzwerkkommunikation und Latenzmanagement notwendig, um Stabilität auch in komplexen Umgebungen zu gewährleisten. Um die Sicherheit der Systeme aufrechtzuerhalten und zu verbessern, raten wir das Führen eines Zeitplans für regelmässige Sicherheitsbewertungen, um mit der sich entwickelnden Bedrohungslandschaft im Bereich der Cybersicherheit Schritt zu halten und neue Schwachstellen zu erkennen, sobald sie auftreten. Zudem erfordern die Erweiterung der Operational Design Domain (ODD) und die Validierung zusätzlicher Szenarien eine intensivere Untersuchung. Die Weiterentwicklung der Fernbedienungsstation (Remote Operation Station) mit Fokus auf Gestaltung ergonomischer Arbeitsumgebungen, der Untersuchung psychologischer und kognitiver Anforderungen der Operatoren für Teleassistenz und Teleoperation bleibt ein weiteres zentrales Thema. Wenn als Basis die reale Führerprüfung in der jeweiligen Kategorie der mittels Teleoperation oder Teleassistenz zu überwachenden/bewegenden Fahrzeuge erfolgreich zu absolvieren ist, bleibt festzulegen, ob und falls ja, welche standardisierten Trainings- und Zertifizierungsprogramme für Operatoren erforderlich sind. Die Harmonisierung internationaler Standards ist essenziell, um Interoperabilität und Sicherheit zu sichern. Die Teleoperation kann zumindest im theoretischen Ansatz global erfolgen, was auch die Frage nach der Qualifikation ausländischer virtueller Fahrzeugführenden aufwirft. Ein kooperativer Ansatz zwischen Forschung, Industrie und Behörden wird empfohlen.

Einfluss auf Normenwerk:

Das Projektkonsortium empfiehlt eine Neubewertung bestehender Normen, insbesondere der Artikel 5.2.1.3, 5.2.2.3 und 5.2.3.3 der UN-Regelung Nr. 152. Insbesondere sollte der Geschwindigkeitsbereich für das Notbremssystem (AEBS) für ROL2 angepasst werden, um eine Aktivierung bei Geschwindigkeiten von nur 1 km/h zu ermöglichen. Durch diese Änderung würde eine kritische Pufferzone (zwischen 0 km/h und 1 km/h) geschaffen, welche es ermöglicht ein Fahrzeug mittels Teleoperation (ROL2) zu deblockieren, wenn es auf ein Hindernis auf seiner Strecke trifft und nicht mittels Teleassistenz (ROL3-ROL5) gelöst werden kann. Eine solche Änderung würde die operative Flexibilität und Sicherheit in verschiedenen Szenarien erhöhen.

Ergänzend könnte die im Projekt entwickelte Taxonomie der Remote Operation Levels (ROLs) sowie die definierten Anforderungen an Latenzzeiten, Cybersecurity und Fernbedienungsstation (Remote Operation Station), in bestehende Normen integriert werden. Szenariobasierte Validierungen bieten zudem Potenzial, Testmethoden für zukünftige Standards zu standardisieren und praxisnah zu gestalten. Dabei sollte der internationale Fortschritt in der Fahrzeugindustrie berücksichtigt werden, um die Interoperabilität zu gewährleisten und sicherzustellen, dass nationale Vorschriften die technologischen Entwicklungen nicht unnötig einschränken.

Der Präsident/die Präsidentin der Begleitkommission:

Name: Neubauer

Vorname: Martin

Amt, Firma, Institut: PostAuto

Unterschrift des Präsidenten/der Präsidentin der Begleitkommission: