REPUBLIC OF ZAMBIA

ROAD TRANSPORT AND SAFETY AGENCY (RTSA)

TRANSPORT CORRIDORS FOR ECONOMIC RESILIENCE (TRACER)

TERMS OF REFERENCE

DESIGN CONSULTANT FOR THE SMART CORRIDOR PROJECT

DAR ES SALAAM CORRIDOR

Employer: Road Transport and Safety Agency (RTSA)

Financing: World Bank

Reference: ZM-RTSA-444824-CS-QCBS

July 2026

Contents

1. Introduction 4
2. Background to the Assignment 4
   2.1 Modular SMART Corridor concept 5
      2.1.1 Traffic Management, Tolling, and Enforcement Module 6
      2.1.2 Border and Trade Facilitation Module 6
      2.1.3 Road Safety and Vulnerable Road User Protection Module 6
      2.1.4 Corridor Entry and Exit Monitoring Module 7
      2.1.5 Integration and Data Management Layer 7
   2.2 Institutional Capacity Building and Inter-Institutional Coordination 8
   2.3 Corridor Infrastructure and Roadside Operational Facilities 8
   2.4 TRACER Project Context 8
3. Objective of the Assignment 8
4. Scope of Work 9
   4.1 Project Management and Coordination 10
   4.2 System Analysis and Detailed Design 10
      4.2.1 Baseline and Existing Systems 10
      4.2.2 Institutional, Legal and Governance 11
      4.2.3 Functional and Technical Design 11
      4.2.4 Corridor Infrastructure and Civil Design 12
      4.2.5 Trade, Payments and Tolling 12
      4.2.6 Phasing, Cost, Operations and Monitoring 13
   4.3 Cybersecurity, Data Protection, and Physical Security of Field Assets 13
   4.4 Training and Documentation 13
   4.5 Maintenance and Support 14
      4.5.1 Sustainability and Long-Term Operability 14
   4.6 Compliance and Standards 15
5. Deliverables and Timeline 15
6. Approach and Methodology 19
7. Reporting and Coordination 20
8. Stakeholder Consultations 20
9. Assignment Duration and Duty Station 20
10. Client Responsibilities and Data 21
   10.1 Facilities and Assistance from the Employer 21
   10.2 Consultant Facilities, Office, Transport, and Field Logistics 21
11. Review, Acceptance, and Performance 21

12. Required Expertise 22
12.1 Consulting Firm Qualification Requirements 22
12.2 Key and Non-Key Experts 22
13. Payment Schedule 28
14. Annex 1. System Design Principles 29
15. Annex 2. Glossary of Terms and Abbreviations 72

1. Introduction

The Government of Zambia is advancing the development of a **SMART (Safety, Mobility, Automated, Real-time Traffic Management) Corridor** along the Dar es Salaam Corridor, specifically the Lusaka–Nakonde section, in order to improve corridor efficiency, road safety, enforcement effectiveness, and trade facilitation through an integrated and interoperable corridor management approach. The initiative is expected to reduce transit times and delays at control points, improve speed and loading compliance, strengthen incident detection and response, and improve the completeness and timeliness of corridor performance data available to participating institutions.

The SMART Corridor is structured around four interrelated pillars adopted by the Project: corridor monitoring, traffic management, trade facilitation, and road safety. Each pillar is delivered through a corresponding functional module, described in the Background and used throughout this Terms of Reference: corridor monitoring through the corridor entry and exit monitoring module; traffic management through the traffic management, tolling and enforcement module; trade facilitation through the border and trade facilitation module; and road safety through the road safety and vulnerable road user protection module.

For the purposes of this Terms of Reference (ToR), the SMART Corridor concept shall be understood as a coordinated system of digital, physical, and operational measures that are planned and operated as one corridor ecosystem rather than as isolated projects. This includes not only platforms, sensors, and communications, but also the supporting roadside and corridor infrastructure, institutional workflows, safe stopping and control facilities, and payment and trade interfaces required for the corridor to function as an integrated operating environment.

The Project responds to the need for a coordinated, multi-agency corridor operating environment in which field systems, institutional workflows, and data platforms function as an integrated whole. The assignment therefore goes beyond equipment definition and shall establish the functional, technical, institutional, and implementation basis for an integrated SMART Corridor system.

The Government of Zambia, with financing from the World Bank under the Transport Corridors for Economic Resilience (TRACER) Project[1] (Project ID: P180801), is therefore seeking to recruit a reputable international firm to undertake the detailed design of the integrated SMART Corridor system.

2. Background to the Assignment

The SMART Corridor initiative is intended to establish an integrated, interoperable, and data-driven corridor operating environment that supports corridor monitoring, road safety, enforcement, tolling and Weigh-in-Motion (WIM) operations, border efficiency, trade facilitation, security, and inter-agency coordination. It is aligned with the TRACER programme and with broader national and regional trade-facilitation and corridor-integration objectives.

For the purposes of this assignment, the Road Transport and Safety Agency (RTSA) shall serve as the Employer and lead contracting agency, unless the Government of Zambia formally designates another entity in writing during the procurement process. RTSA is a statutory body established

[1]https://documents1.worldbank.org/curated/en/099013124091024437/pdf/BOSIB115c56da804a19bb31df94743849b1.pdf

under the Road Traffic Act No. 11 of 2002, responsible for implementing Government policy on road safety and transport management.

The SMART Corridor is conceived primarily as an intelligent transport systems and digital transformation initiative rather than as a conventional road infrastructure project, while recognising that targeted enabling civil works are required to support the installation and operation of corridor technologies and associated operational facilities.

The corridor presents a set of conditions that shape the design. Roadside monitoring and enforcement infrastructure already exists in places and may provide a basis for integration. Toll plazas, police checkpoints and weighbridge functions sit in operational proximity to one another, which supports the concept of integrated corridor control portals. Much of the route is single carriageway, with roadside activity, village environments and significant pedestrian exposure, which together make digitally enabled safety, enforcement and speed-management measures a priority. There is a recognised need for remote visibility of corridor control points, greater transparency of weighbridge and enforcement operations, and a centralised data environment capable of supporting multi-agency monitoring and decision-making from Lusaka.

2.1 Modular SMART Corridor concept

At its core, the SMART Corridor aims to establish a coherent ITS ecosystem that enables real-time monitoring and management of corridor operations. This ecosystem is expected to integrate multiple functional domains, including traffic management, enforcement, border processes, safety monitoring, and security, while respecting the institutional mandates of the different agencies involved.

Rather than creating a single, centralized operational system for all functions, the project promotes multiple functional systems, managed by different agencies according to their mandates, but fully interoperable and able to exchange data. This approach reflects both institutional realities and international best practice, and aims to:

i) avoid duplication of existing or ongoing systems (such as the ECTS under ZATP-II);
ii) leverage prior investments already made by different agencies;
iii) ensure scalability and flexibility, allowing new modules to be added over time.

The concept therefore foresees a modular architecture, in which different technological layers support distinct operational functions while feeding into a common data environment. Four functional modules are central to the SMART Corridor concept:

i) **Traffic management, tolling, and enforcement modules**, including toll plazas, weigh-in-motion, speed enforcement, and police operations;
ii) **Border and trade facilitation modules**, aligned with One-Stop Border Post (or Non-Stop- Border Stop) operations and existing customs platforms;
iii) **Road safety and vulnerable road user protection modules**, particularly in village sections and high-accident locations;
iv) **Corridor entry and exit monitoring**, enabling visibility of vehicle movements into and out of the corridor for enforcement, safety, and trade purposes.

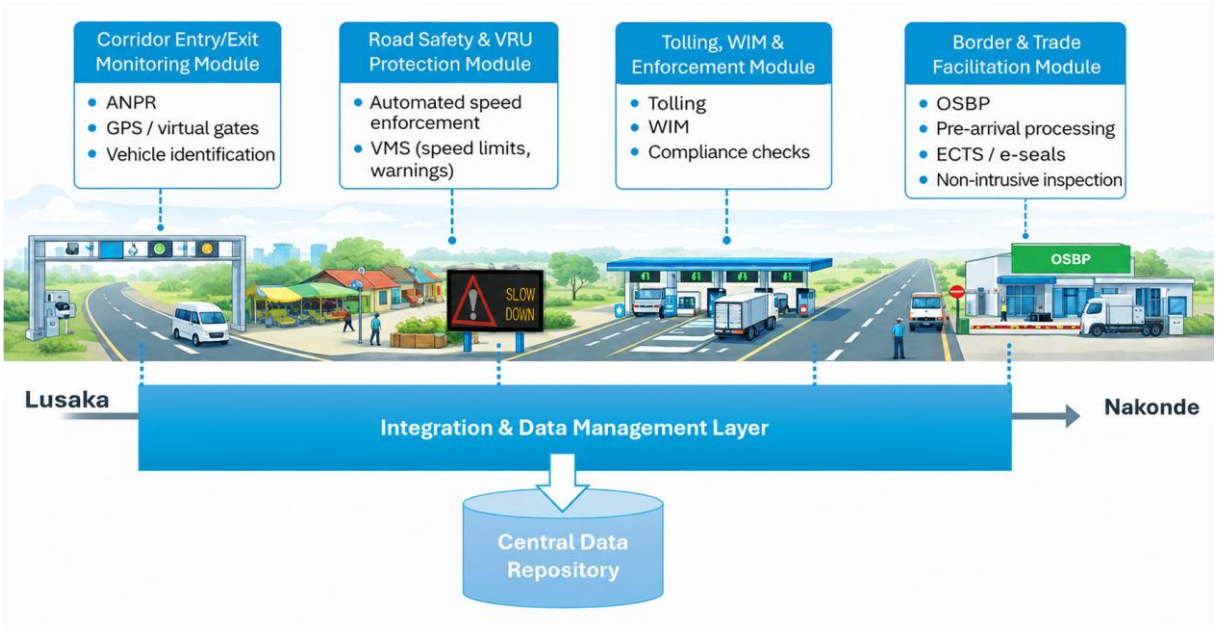

Figure 1: Conceptual illustration of SMART Corridor functional modules along the corridor

All four functional modules shall be supported by **a common Integration and Data Management Layer**, enabling data-sharing, coordinated decision-making, corridor-wide performance monitoring, and differentiated role-based access for participating institutions through a central data repository and operational control capability.

2.1.1 Traffic Management, Tolling, and Enforcement Module

This module covers the corridor control points at which compliance, enforcement and traffic-flow management converge: toll plazas, weigh-in-motion and weighbridge stations, speed and ANPR enforcement sites, and police checkpoints. The operating intent is that these are treated as functionally integrated control portals rather than as a succession of separate stops, so that corridor throughput improves while enforcement becomes risk-based and evidentially sound. It is also the point at which vehicle compliance records, including registration, licensing, insurance, inspection and permits, become available to enforcement processes, subject to the data governance and access arrangements agreed between the participating agencies. Detailed requirements are set out in Annex 1.

2.1.2 Border and Trade Facilitation Module

This module addresses trade facilitation and border efficiency along the corridor, aligned with One-Stop Border Post operations and with the customs platforms already in service. Its purpose is to reduce clearance times through pre-arrival information submission, risk management and coordinated inspection, and to connect corridor systems to customs workflows, transit monitoring, permits, tolling and inspection so that a consignment is handled as a single movement rather than a series of unconnected events. The SMART Corridor does not procure a separate cargo tracking capability; the module aligns with and builds on the Electronic Cargo Tracking System implemented under ZATP-II. Detailed requirements are set out in Annex 1.

2.1.3 Road Safety and Vulnerable Road User Protection Module

This module addresses safety outcomes along the corridor, with particular attention to village sections, built-up environments, roadside activity zones and locations with a recorded concentra-

tion of crashes. It combines speed compliance and enforcement technology with incident detection, emergency response coordination and post-crash workflow, and it is the module through which corridor safety data becomes usable for road safety audit, hotspot identification and the prioritisation of physical interventions. A corridor blackspot treatment framework, linking analytics to field measures such as markings, signing, pedestrian crossings and traffic calming, forms part of this module. Detailed requirements are set out in Annex 1.

2.1.4 Corridor Entry and Exit Monitoring Module

This module provides visibility of vehicle movements into and out of the corridor, drawing on data feeds from toll plazas, weighbridge and weigh-in-motion stations, enforcement points and border-related systems. It supports corridor performance measurement, including travel times, delays at control points, compliance rates and incident response times, and it enables origin-destination and corridor journey analysis by linking observations across control points. It is the basis for the corridor observatory function, through which dashboards and periodic performance summaries are made available to participating institutions. Detailed requirements are set out in Annex 1.

2.1.5 Integration and Data Management Layer

Each functional module addresses a distinct operational domain, but the effectiveness of the SMART Corridor depends on a common integration and data management layer beneath them. Operational platforms remain agency-managed; the integration layer aggregates data from them into a central repository and control capability supporting geospatial visualisation, corridor-wide performance monitoring, agency-specific dashboards and evidence-based planning. It is defined by open standards, published interfaces and harmonised data definitions, so that modules interoperate, further modules and geographic lots can be added without disruption, and the corridor remains able to connect to national and regional platforms and to accommodate later technologies. Operational continuity, including power reliability, connectivity resilience, cybersecurity and access control, is a property of this layer rather than of any single module. Detailed requirements are set out in Annex 1.

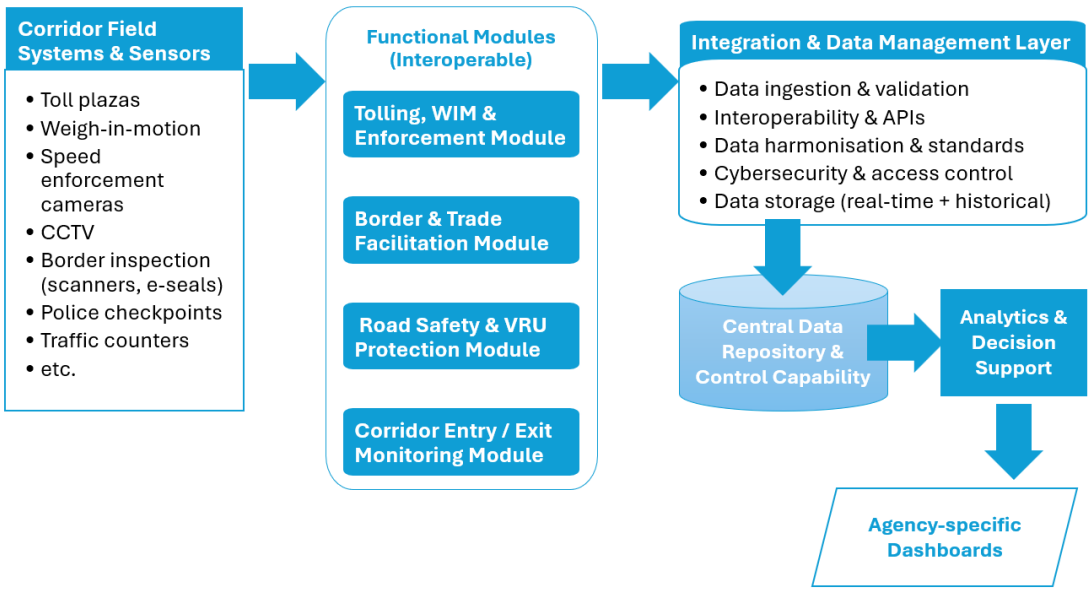

Figure 2: SMART Corridor integrated ITS architecture

2.2 Institutional Capacity Building and Inter-Institutional Coordination

The SMART Corridor is a multi-agency undertaking, and its operation depends as much on institutional arrangements as on technology. It requires an operational governance model covering data ownership, command and escalation hierarchy, incident authority, enforcement workflow responsibility and formalised data-sharing between agencies, together with the operational capacity, skills and maintenance arrangements needed to run and sustain the systems once delivered. The Consultant's responsibilities for institutional analysis and capacity-building recommendations are set out under Scope of Work.

2.3 Corridor Infrastructure and Roadside Operational Facilities

The SMART Corridor concept requires digital systems to be translated into implementable corridor infrastructure and roadside operational facilities, including gantries, enforcement and control sites, weighbridge and inspection areas, communications routes and power provision. These interface with road geometry, pavement condition, traffic operations, safety, maintenance access, fibre ducting and land requirements, and the design work under this assignment treats them as a single problem rather than as separate civil and digital exercises.

2.4 TRACER Project Context

The Consultant shall take into account the wider TRACER project context, including the Project development objective, the relevant corridor-improvement components, and the intended relationship between SMART Corridor investments and associated road, border, logistics, safety, and institutional strengthening measures under the broader programme.

3. Objective of the Assignment

The primary objective of this assignment is to conduct a detailed functional, technical, institutional, and implementation-ready design of the integrated SMART Corridor system for the Dar es Salaam Corridor (Lusaka–Nakonde section). This scope includes the development of comprehensive technical specifications, detailed cost estimates, and a phased implementation plan from both technological and geographical perspectives. It also covers rollout planning, procurement packaging strategies, and well-defined recommendations for institutional arrangements, as well as operations, maintenance, and long-term sustainability.

More specifically, the Design Consultant shall define how the SMART Corridor will function as a coherent multi-agency operating ecosystem aligned with the TRACER Project goals. This shall include, but not limited to:

i) The development of a comprehensive system architecture, together with concept design for roadside infrastructure across the corridor and detailed engineering design to tender-ready standard for the sites comprising the first deployment phase;

ii) The definition of operational concepts and unified user roles;

iii) The establishment of inter-agency interfaces and data-sharing protocols;

iv) The identification of implementation priorities, and a robust procurement-ready documentation package (including tender documents for supply and installation);

v) The formulation of sustainability arrangements to ensure the corridor remains operational and technologically relevant over its lifecycle.

vi) A phased implementation plan, covering both technical aspects (e.g., prioritization of modules/functions) and geographical deployment (e.g., geographic lots).

4. Scope of Work

The Design Consultant shall prepare a complete and coherent design package for an integrated SMART Corridor system for the Dar es Salaam Corridor (Lusaka–Nakonde section). The assignment shall be deliverable-driven and shall include planning, analysis, design, cost estimation, implementation phasing, institutional arrangements, and the preparation of tender-ready procurement documentation for implementation.

The assignment shall be structured around four functional modules:

i) Traffic management, tolling, and enforcement;

ii) Border and trade facilitation;

iii) Road safety and Vulnerable Road User (VRU) protection;

iv) Corridor entry and exit monitoring.

A different module structure may be proposed, provided it is duly justified.

For the purposes of field work, survey and design, the Lusaka–Nakonde section of the Dar es Salaam Corridor is approximately 1,020 km in length along the Great North Road, comprising Lusaka–Serenje (approximately 360 km), Serenje–Mpika (approximately 203 km), Mpika–Chinsali (approximately 228 km) and Chinsali–Nakonde (approximately 226 km). These distances are indicative and shall be confirmed by the Consultant during the baseline assessment.

A distinction shall be maintained throughout between the design of the system and the scope of its funded deployment. The system architecture, data model, interface definitions, data governance and institutional arrangements shall be developed for the corridor as a whole, so that the design remains coherent and extensible and so that further modules, geographic lots and later technologies can be added without architectural redesign. Site design, the phased implementation plan and the cost estimate shall be developed against the funded implementation scope for each pillar, site design being taken to concept level across that scope and to tender-ready level only for the sites comprising Phase 1, as set out under System Analysis and Detailed Design. The funded scope differs by pillar: corridor monitoring along the Lusaka–Nakonde corridor; traffic management along the Lusaka–Nakonde corridor and the Serenje–Mpika section; trade facilitation at Nakonde and along the Lusaka–Nakonde corridor, extending beyond the corridor only in respect of interoperability with regional, cross-border and transit systems; and road safety on the Serenje–Mpika section. The Consultant shall validate this scope with the Employer during inception, and shall identify separately any scope that would require financing beyond the present Project.

For each module, and for the cross-cutting Integration and Data Management Layer, the Consultant shall define, including but not limited to, the operational purpose; institutions and user groups; key operational workflows and use cases; required field, communications, platform, and data components; interoperability among corridor functions and interfaces with existing and planned systems; data ownership, access rights, and governance requirements; system ownership, hosting model, operating arrangements, and operations and maintenance responsibilities; operational staffing, budget, and recurrent cost requirements, including financing assumptions beyond the project period; and implementation assumptions, dependencies, risks, and capital cost implications.

The Consultant shall prepare an operationalization plan for the integrated SMART Corridor system, including recommendations on institutional arrangements, system hosting, day-to-day operations, long-term maintenance, data governance across agencies, and sustainability of recurrent costs such as hosting, licenses, upgrades, connectivity, and cybersecurity.

The Consultant shall also prepare a comprehensive procurement strategy for implementation, including recommendations on the optimal packaging of works, goods, software, systems integration, communications infrastructure, and related services into manageable and market-appropriate tender packages (e.g., separating civil works from system integration where appropriate) rather than assuming a single turnkey contract.

The functional and technical requirements set out in Annex 1, System Design Principles, are indicative. They convey the scope and ambition sought and are intended to guide the Consultant's analysis. The Consultant shall validate, refine and complete them on the basis of the baseline assessment, stakeholder consultations and the design work carried out under this assignment.

The Consultant shall therefore treat this assignment as the design of a multi-agency digital-physical transport corridor operating ecosystem rather than as the design of a standalone traffic control system. The design package shall be fully procurement-ready and shall clearly show how corridor infrastructure, digital systems, institutional arrangements, and operational workflows fit together.

4.1 Project Management and Coordination

The Consultant's project management and coordination obligations under this assignment shall include, but not be limited to:

i) Establishment of a dedicated project management team;
ii) Preparation of a detailed Project Implementation Plan (PIP);
iii) Definition of milestones, timelines, and resource allocation;
iv) Regular coordination meetings with the Employer, stakeholders and the Technical Advisor;
v) Risk identification, mitigation planning, and progress reporting;
vi) Quality assurance and quality control procedures.

4.2 System Analysis and Detailed Design

The system analysis and detailed design work shall include, but not be limited to:

4.2.1 Baseline and Existing Systems

i) Review of existing corridor infrastructure and ITS assets, including current and planned RDA WIM installations and any traffic-monitoring, camera or weighbridge installations implemented or planned under corridor concession arrangements, to ensure non-duplication, compatibility and integration, and to leverage existing investments where practicable;
ii) Detailed corridor analysis, including traffic, safety, climate vulnerability (flood/washaway risks), and environmental conditions;
iii) Assessment of existing fibre-optic infrastructure along the corridor and identification of new fibre or alternative communications requirements (e.g., satellite or microwave back-up) where existing connectivity is absent or insufficient;
iv) Assessment of corridor road asset inventory and asset-condition monitoring opportunities, including use of camera or vehicle-based sensing where appropriate;

4.2.2 Institutional, Legal and Governance

i) Analysis of the institutional framework and data sharing processes among the different agencies/ministries (RTSA, RDA, ZRA, Police, etc.);

ii) Mapping of the mandates, roles, and responsibilities of participating Government of the Republic of Zambia (GRZ) institutions and other public entities relevant to corridor operations, implementation, regulation, data ownership, and long-term operations, covering, including but not limited to, RTSA, the Road Development Agency (RDA), the Zambia Revenue Authority (ZRA), police and enforcement bodies, toll and weighbridge operators, local authorities, emergency-response institutions, and any additional entities designated by the Employer;

iii) Review of the applicable legal and regulatory framework, including the enabling Acts, regulations, statutory instruments, and operating mandates relevant to corridor monitoring, road management, tolling, axle-load control, transport regulation, customs and border management, enforcement, data protection, and cybersecurity, and identification of any legal, regulatory, or procedural adjustments, including inter-agency data-sharing agreements, required to operationalise the proposed SMART Corridor arrangements;

iv) Assessment of the institutional, legal, and contractual implications of future tolling arrangements, including consultation requirements with the tolling authority and other affected institutions, and of existing or planned PPP and concession road sections and their implications for interoperability, revenue processes, system governance, and future corridor expansion;

v) Definition of the institutional framework and data sharing process after the project implementation;

vi) Preparation of an Operational Governance Model covering command hierarchy, incident authority, enforcement workflow chain, inter-agency escalation paths, data ownership, hosting responsibilities, maintenance responsibilities, and sustainable post-implementation operating arrangements;

4.2.3 Functional and Technical Design

i) Definition of functional and technical system requirements, including, for each lot, segment and major activity area, the principal data types, interfaces and expected outputs;

ii) Preparation of system architecture and subsystem interfaces utilizing open standards and APIs;

iii) Network, cybersecurity, and data flow design;

iv) Assessment of physical security requirements for ITS field assets, including site selection, protective enclosures, tamper detection, resilience of power and communications, and integration of physical security alerts with system monitoring;

v) Assessment of UAV/drone use cases for corridor monitoring and post-crash management, including type, basing/station locations, operating concept, data transmission, and regulatory implications, where justified;

4.2.4 Corridor Infrastructure and Civil Design

i) Preparation of design documentation to two levels of detail: concept layouts and design criteria for the corridor as a whole, and detailed design documents and engineering drawings (civil, structural, electrical and telecommunications) to a standard suitable for tendering, for the sites comprising the first deployment phase (Phase 1) as confirmed under Deliverable 3. At both levels the documentation shall cover roadside stations, WIM plazas, enforcement bays, safe stopping areas, selected driver-rest or emergency-response support facilities where required, control centre buildings or rooms, power supply arrangements, fibre ducting, equipment foundations, gantries, poles and communications masts;

ii) Assessment of pavement structural integrity for any proposed pavement-integrated sensors (e.g., WIM) to ensure compatibility with Zambian axle-load classes and pavement design standards, and to prevent premature pavement failure;

iii) Assessment of traffic flow and queue-management measures around WIM/weighbridge areas, including geometric, operational, and ITS measures;

iv) Coordination of the design with road upgrading works being undertaken along the corridor under the wider TRACER Project, including the Serenje–Mpika section. The Consultant shall identify where roadside installations, foundations, ducting, power and communications routing fall within sections programmed for reconstruction, shall avoid designing fixed installations into sections due to be rebuilt, and shall identify opportunities to install ducting, foundations and enabling works in advance as part of those works, at lower cost and without subsequent disturbance to new pavement. The Consultant shall also sequence the design and installation of the trade facilitation and border-related elements against the development of the Nakonde One-Stop Border Post, so that corridor systems and border infrastructure are delivered in a compatible order and without duplication;

4.2.5 Trade, Payments and Tolling

i) Preparation of a Corridor Digital Trade Architecture showing how customs, ECTS, OSBP workflows, permits, inspections, tolling, WIM, enforcement, and data-sharing processes shall interoperate across the corridor without unnecessary duplication of existing systems;

ii) Support to the definition and harmonisation of the documents and information required for cross-border movements along the corridor, in coordination with the responsible border and customs institutions;

iii) Preparation of a Unified Corridor Payment Platform concept, including design principles for multi-agency payment interfaces, payment-confirmation workflows, penalties, permit fees, weighbridge-related charges, border charges where applicable, reconciliation, and single-clearing or equivalent settlement arrangements, taking into account national payment and financial-control requirements;

iv) Design provisions for e-tolling / automatic toll collection, including the definition of future-ready infrastructure where deployment is deferred. The Consultant shall determine, as part of the prioritisation analysis, which elements of automatic toll collection fall within the funded scope and which require passive provision only;

v) Review and propose the automation of corridor control and revenue-related systems, including weighbridge and weighbridge-station operations, taking into account related automation and financial-management initiatives of the National Road Fund

Agency (NRFA), and define an integration approach that avoids duplication of existing or ongoing investments;[2]

4.2.6 Phasing, Cost, Operations and Monitoring

i) Preparation of a phased prioritisation framework, comprising Phase 1 and such subsequent phases as the analysis supports, together with prioritisation criteria, cost-benefit ranking of subsystems and sites, and clear triggers and dependencies for expansion;

ii) Definition of system ownership, hosting, operating model, staffing, maintenance, and recurrent cost arrangements;

iii) Preparation of a corridor monitoring and evaluation framework, including baseline indicators, before/after assessment logic, and measurable corridor KPIs for safety, operations, compliance, trade facilitation, and institutional performance;

4.3 Cybersecurity, Data Protection, and Physical Security of Field Assets

The Consultant shall define the cybersecurity, data protection and physical security requirements to be met by the SMART Corridor system and carried into the procurement documentation. These shall address, as a minimum and without limitation:

i) Encrypted communications;

ii) Secure authentication and authorization;

iii) Role-based access control;

iv) Audit logs and system monitoring;

v) Compliance with national and international data protection regulations;

vi) Secure siting and protective enclosure requirements for cameras, sensors, WIM equipment, VMS, roadside cabinets, power systems, and communications assets;

vii) Tamper detection, fault monitoring, and alerting arrangements for critical roadside equipment;

viii) Power and communications resilience measures to reduce outage and vandalism risks;

ix) Integration of physical security events with central monitoring, maintenance, and incident management workflows.

4.4 Training and Documentation

Training and documentation provisions under this assignment shall focus on i) on-the-job knowledge transfer to selected Government staff on the SMART Corridor design and ii) the definition of procurement requirements for future vendor-delivered manuals, training materials, and training services. This assignment shall not include full-scale execution of institutional capacity-

[2] NRFA operates a tailor-made financial management system which is not currently integrated with its tolls management and contract management systems. NRFA is upgrading the system to improve financial reporting, strengthen the capture of road funding data and support strategic decision-making, and has partially integrated it with the Road Development Agency for electronic submission of payment documentation. Detailed scoping of the upgrade has not yet been completed.

building programmes or preparation of final solution-specific manuals for the implemented system.

The scope shall include:

i) On-the-job knowledge transfer for designated Government staff covering the design assumptions, architecture, operational concepts, phasing logic, and institutional arrangements of the SMART Corridor;

ii) Capacity-building needs assessment and recommendations identifying the priority institutions, topics, delivery formats, and sequencing for future implementation-phase training;

iii) Definition of minimum vendor obligations for user manuals, administrator guides, operations and maintenance manuals, and training materials, including languages, accessibility, formats, and minimum content standards;

iv) Definition of minimum training outcomes, participant groups, delivery requirements, and evaluation criteria to be included in the procurement documentation for implementation vendor(s);

v) Definition of acceptance criteria, completion records, and sign-off procedures for vendor-delivered manuals and training during future implementation;

vi) Template outlines or minimum content requirements for Standard Operating Procedures (SOPs) and operational guidelines to be finalised by the selected implementation vendor(s).

4.5 Maintenance and Support

Under this assignment, the Design Consultant shall define the minimum warranty, maintenance, support, spare parts, update/patching, service-level, and handover requirements to be included in the future tender documents and implementation contracts. The Consultant shall also define the corresponding institutional responsibilities, recurrent cost implications, and performance monitoring arrangements for the post-implementation period.

The requirements shall include:

i) Minimum warranty period and defects-liability requirements;

ii) Preventive and corrective maintenance scope during the warranty/support period;

iii) Software updates, cybersecurity patches, and version-management obligations;

iv) Service-level agreements (SLAs), escalation paths, and support channels;

v) Defined response and restoration times for critical and non-critical failures;

vi) Handover, stabilization, knowledge-transfer, and transition-to-operations requirements.

4.5.1 Sustainability and Long-Term Operability

The Consultant shall assess and document the sustainability of the proposed SMART Corridor arrangements, including affordability of recurrent costs, maintainability of field and central assets, institutional capacity for operations, replacement cycles, spare-parts strategy, utility and connectivity dependencies, lifecycle risks, and practical measures required to keep the system operational over the long term.

This assessment shall identify the minimum operational model, staffing assumptions, budgetary implications, and sustainability risks that should be considered by the Government before implementation and during subsequent operations.

4.6 Compliance and Standards

The design and the resulting procurement documentation shall demonstrate, and shall require of the implementation vendor, the following:

i) Compliance with national traffic, safety, customs, border-operation, and data protection regulations;

ii) Alignment with international ITS standards (e.g., ISO, IEEE, CEN/TC 278) and best practices;

iii) Documentation of compliance and certification where required;

iv) Alignment, where relevant, with bilateral and multilateral corridor agreements, One-Stop Border Post (OSBP) arrangements, transit-data-sharing instruments, and other inter-governmental protocols applicable to cross-border operations.

5. Deliverables and Timeline

The Design Consultant shall prepare and submit the deliverables set out in Table 1.

Table 1: Schedule of Deliverables

Period	Deliverable	Scope	Milestone
Month 1	Deliverable 1 (D1): Inception Report and Design Phase Work Plan	This report shall confirm the Consultant's understanding of the assignment and present the refined methodology, detailed work plan, stakeholder engagement approach, schedule, and quality assurance arrangements for the design phase.	Final at the end of Month 1
Months 2-3	Deliverable 2 (D2): Corridor Analysis and Baseline Assessment Report	This report shall present the assessment of corridor conditions, covering: i) traffic operations, enforcement practices and road safety conditions; ii) toll plazas, weighbridges and border-related processes; iii) power and connectivity constraints; iv) a mapping of existing digital and ITS systems operated by corridor stakeholders; v) a baseline assessment of existing fibre-optic and communications infrastructure; vi) a preliminary review of physical security risks for field assets; vii) the feasibility of UAV/drone use cases where justified; viii) blackspots and priority safety-improvement locations; ix) existing or required safe-stopping and roadside operational facilities;	Draft at the end of Month 2; Final at the end of Month 3

Period	Deliverable	Scope	Milestone
		x) the initial monitoring and evaluation baseline against which corridor improvements can later be assessed.	
Months 4-6	Deliverable 3 (D3): Functional, Technical and Institutional Design Report	This report shall define: i) the functional design of the SMART Corridor; ii) the modular and interoperable system architecture, data flows and integration principles; iii) institutional roles and responsibilities, and inter-agency coordination mechanisms; iv) operationalization arrangements, system ownership and hosting approach, and the operations and maintenance model; v) data governance arrangements and cybersecurity requirements; vi) the corridor infrastructure and civil design basis for key field sites and facilities; vii) the Corridor Digital Trade Architecture; viii) the Unified Corridor Payment Platform concept; ix) the Operational Governance Model for post-implementation operations; x) a high-level data dictionary / data-output matrix showing the key data types, interfaces, intended users, and expected outputs by module and, where applicable, by corridor segment or lot. The Consultant shall confirm, as part of this deliverable, the scope of the first deployment phase (Phase 1), in order to enable preparation of the corresponding tender package. The Consultant shall determine what Phase 1 comprises and shall justify that determination against the baseline assessment, the technical dependencies between subsystems, and the prioritisation and cost-benefit analysis to be developed under Deliverable 4. In doing so the Consultant shall satisfy two requirements set by the Employer: that Phase 1 be capable of being tendered on the basis of the design completed by the end of Month 9, and therefore not dependent on design work concluding later in the assignment; and that the early award of Phase 1 materially shorten the overall implementation programme. Subsequent phases shall also fall within the Project implementation period, and	Draft at the end of Month 5; Final at the end of Month 6

Period	Deliverable	Scope	Milestone
		phases shall not be assumed to run consecutively where dependencies permit them to overlap. The full sequencing, costing and prioritisation framework shall be completed under Deliverable 4. Any extension of geographic coverage or scope beyond that funded under the present Project shall be presented separately, as a pipeline for future financing, and shall not be described as a phase of this Project.	
Months 7-9	Deliverable 4 (D4): Phased Implementation Strategy and Cost Estimate	This report shall define the phased implementation approach, comprising: i) alternative packages and scenarios matched to different financing envelopes; ii) geographical lots or corridor segments, and the allocation of functional modules per lot; iii) implementation sequencing based on criticality, and the geographic coverage of each package; iv) institutional capacity measures accompanying each phase; v) procurement packaging recommendations; vi) detailed capital and recurrent cost estimates disaggregated by geographical lot, functional module and major cost component, including key assumptions; vii) the deployment logic for Phase 1 and for each subsequent phase proposed, the number of phases being determined by the Consultant's analysis rather than assumed; viii) cost-benefit ranking of subsystems and sites; ix) the monitoring and evaluation framework to be used for before and after assessment of implementation results. The strategy shall be tested for deliverability against the time available, and not against funding alone. The Consultant shall prepare an implementation programme showing, for each phase and lot, the procurement lead time, contract duration, installation sequence and commissioning period, demonstrated against the Project closing date, currently 27 February 2030, as confirmed by the Employer during inception. Where the analysis shows that any element of the funded scope cannot be procured, installed and commissioned before that date, the Consultant shall identify it explicitly, quantify	Draft at the end of Month 8; Final at the end of Month 9

Period	Deliverable	Scope	Milestone
		it, and set out the options available to the Employer, including re-scoping, re-sequencing, earlier packaging, or deferral to future financing. The Consultant shall further state and justify how detailed design for each phase beyond Phase 1 is to be delivered, whether by the implementation contractor against the Employer's requirements and specifications, by a subsequent design assignment, or otherwise. The cost estimate shall include the cost of that design work wherever it is to sit, and the implementation programme shall reflect any procurement required to secure it. Deliverable 5 shall structure the tender documentation accordingly.	
Months 6-12	Deliverable 5 (D5): Procurement Strategy and Tender Documentation for Implementation	This deliverable shall consist of the preparation of a procurement strategy and a complete set of procurement-ready tender documents / technical specifications for the selection of the firm(s) responsible for implementation of the SMART Corridor. The tender documentation shall cover the entire funded implementation scope and not Phase 1 alone. The Phase 1 package delivered at the end of Month 9 is an early package within that scope, and the form of documentation for scope beyond Phase 1 shall follow from the design delivery model determined under Deliverable 4. Drafting of procurement inputs shall commence progressively as the assignment develops, drawing from the outputs of Deliverable 3 and Deliverable 4, and shall be consolidated into a final procurement package at the end of the assignment. The deliverable shall: i) recommend packaging into manageable and market-appropriate lots; ii) define interface responsibilities where multiple contractors are envisaged; iii) include mandatory requirements for vendor-delivered user manuals, training materials, training completion, acceptance criteria and sign-off procedures; iv) address packages for civil works, roadside and field equipment, communications infrastructure, platforms and software, systems integration, and support services, together with interface and interoperability rules across packages.	Progressive drafting from Month 6 onward; procurement-ready tender package for Phase 1 at the end of Month 9; draft package at the end of Month 11; final at the end of Month 12

Period	Deliverable	Scope	Milestone
Months 10-12	Deliverable 6 (D6): Final Design Consolidation and Handover Report	This report shall consolidate and finalise all design outputs produced during the assignment into a single, coherent, and internally consistent design package. It shall confirm that comments received from RTSA, corridor stakeholders, and the Technical Advisor / Advisory Consultant have been appropriately addressed across all previous deliverables.	Draft at the end of Month 11; Final at the end of Month 12
Months 1-12	On-the-Job Knowledge Transfer and Capacity Building Recommendations	The Consultant shall provide light-touch on-the-job knowledge transfer to designated Government staff on the SMART Corridor design and shall prepare recommendations for future institutional capacity building to be implemented later under the implementation phase. This work shall not include the execution of full-scale institutional training programmes.	Continuous (light-touch) throughout the assignment

6. Approach and Methodology

The Consultant shall propose a robust and practical methodology covering, including but not limited to, inception, baseline assessment, stakeholder engagement, operational needs analysis, inventory and assessment of existing systems, functional and technical design, institutional and governance design, implementation phasing, procurement packaging, costing, and handover of procurement-ready documentation.

The methodology shall demonstrate how the Consultant will address interoperability across SMART Corridor modules, road engineering and field installation constraints, physical security of field assets, communications and fibre-optic requirements, and the preparation of alternative implementation scenarios aligned with different financing envelopes.

The methodology shall state the number of corridor sites, control points and corridor segments the Consultant has assumed for the purposes of field work, survey and detailed site design, together with the basis for that assumption. The Consultant shall not treat the assumed figure as a limit on the work required, and shall identify the mechanism by which it would be reconciled with the findings of the baseline assessment. The methodology shall further state the scope the Consultant expects the Phase 1 tender package to comprise, and the reasoning for it, recognising that Phase 1 is to be determined under Deliverable 3 and that the expectation stated in the proposal is not binding on that determination. The methodology shall further state how the Consultant expects detailed design for phases beyond Phase 1 to be delivered, and the reasoning for it, on the same non-binding basis. The methodology may be refined during the inception phase, subject to the Employer's review and approval.

In conducting the activities above, the Consultant shall refer to other Bank-financed projects to ensure that the proposed system under this project does not duplicate initiatives, systems, or activities conducted under other World Bank and/or Government financed projects. In particular, a review shall be made of, but not limited to, the Zambia Agribusiness and Trade Project Phase 2 (ZATP-2), the ZRA-driven programme to introduce ASYCUDA World, and ongoing Cross-Border Management (CBM) programmes.

7. Reporting and Coordination

The Design Consultant shall report to the Employer, namely the Road Transport and Safety Agency (RTSA), and to the Firm appointed as Technical Advisor for the Smart Corridor Project, which shall be selected through a dedicated tender process, and/or to any other client representative or project management structure as the Employer may formally designate.

The Consultant shall prepare brief monthly progress reports, participate in regular coordination meetings, and promptly flag risks, decisions, dependencies, and actions required from the Employer or stakeholders.

Reporting shall clearly identify completed activities, upcoming activities, decisions required, stakeholder issues, data gaps, field constraints, risks to schedule or quality, and actions expected from the Employer or other stakeholders.

Where a Steering Committee, Technical Working Group, or equivalent coordination body is established, the Consultant shall support meetings, present findings, and incorporate agreed actions into subsequent deliverables.

Draft and final deliverables shall be submitted to the Employer and to the Technical Advisor / Advisory Consultant in parallel. The Technical Advisor / Advisory Consultant shall provide technical review input to the Employer, while formal acceptance of deliverables shall remain the responsibility of the Employer.

8. Stakeholder Consultations

The Consultant shall undertake structured consultations with corridor stakeholders to identify operational requirements, existing systems, institutional mandates, data-sharing constraints, implementation dependencies, and sustainability considerations.

Stakeholders to be consulted shall include, but not be limited to, RTSA, the Road Development Agency (RDA), the National Road Fund Agency (NRFA), other road and corridor infrastructure authorities, border and trade facilitation institutions, Zambia Revenue Authority, Police and enforcement bodies, toll and weighbridge operators, concessionaires where relevant, utilities/connectivity providers, emergency-response institutions, local authorities, and any other entities designated by the Employer.

The Consultant shall reflect stakeholder consultations in the inception methodology and shall document how stakeholder comments have been addressed in each major deliverable. The Consultant shall also convene a technical validation session with the Employer, the Technical Advisor and the participating institutions at each major deliverable, and for the Phase 1 tender package at Month 9, so that reviewing institutions are able to interrogate and accept the design on an informed basis.

9. Assignment Duration and Duty Station

The expected duration of the assignment is twelve (12) months from contract commencement, unless otherwise agreed by the Employer.

The primary duty station shall be Lusaka, with regular field missions along the Dar es Salaam Corridor (Lusaka–Nakonde section) and to relevant stakeholder locations, installations, border-related facilities, toll plazas, weighbridges, and other sites required for the proper execution of the assignment. Not less than 70% of the total input of the Key and Non-Key Experts listed in these

Terms of Reference shall be delivered in Zambia. This requirement may be met by experts based internationally, regionally or in Zambia. The Consultant shall state in its proposal the assumed distribution of input between internationally based experts and nationally or regionally based experts, and shall show in-country presence by position and by month in its staffing schedule.

10. Client Responsibilities and Data

10.1 Facilities and Assistance from the Employer

The Employer shall facilitate reasonable access to available background documents, corridor studies, site access permissions, stakeholder focal points, and existing data relevant to the assignment, subject to applicable confidentiality, security, and legal constraints.

The Consultant shall be responsible for reviewing, validating, and supplementing the information made available by the Employer and stakeholders. The Consultant shall identify any critical data gaps early and propose practical measures for addressing them.

Any sensitive or restricted data shared for the purposes of the assignment shall be handled in accordance with applicable legal, institutional, cybersecurity, and confidentiality requirements.

10.2 Consultant Facilities, Office, Transport, and Field Logistics

Unless otherwise expressly stated in the Contract, the Consultant shall be responsible for providing its own office accommodation, transport, field mobility, communications, survey tools, IT equipment, staff subsistence, and all other resources required for proper execution of the assignment.

Where site access letters, introductions, coordinated meetings, or security-related clearances are required, the Employer shall provide reasonable facilitation; however, the Consultant shall remain responsible for planning and mobilising the operational resources needed to undertake field work safely and efficiently.

11. Review, Acceptance, and Performance

For each deliverable, the Consultant shall submit a draft version for review, address consolidated comments received from the Employer and the Technical Advisor / Advisory Consultant, and then submit a final version for acceptance.

Designs shall be approved by the Employer, following review and certification by the Technical Advisor, prior to implementation.

The Consultant's performance shall be assessed against the quality, completeness, practicality, timeliness, and internal consistency of deliverables; responsiveness to review comments; effectiveness of stakeholder engagement; and the extent to which the outputs are procurement-ready and operationally implementable.

The Employer may request reasonable clarifications and revisions necessary to achieve an acceptable and internally consistent final design package in accordance with these Terms of Reference and the signed contract.

12. Required Expertise

The Design Consultant shall mobilise a multidisciplinary team with proven experience in the planning and design of complex, multi-agency ITS and corridor-modernisation projects. The team shall collectively cover corridor-level traffic management and transport planning, system architecture and integration, business and system requirements analysis, enforcement and compliance systems, border and trade facilitation digitalisation, digital payments and revenue-system integration, road / civil engineering for field deployments, road safety and emergency-response planning, cybersecurity and data governance, telecommunications and connectivity design, legal, institutional and regulatory analysis, capital and recurrent cost estimation, procurement and tender documentation, and operational coordination.

12.1 Consulting Firm Qualification Requirements

The Consultant shall be a reputable firm, or a joint venture of firms, meeting the following minimum requirements:

i) The firm shall have a minimum of 10 years of proven experience in the planning, design, or implementation of intelligent transport systems, corridor modernisation, or comparable multi-agency technology programmes.

ii) The firm shall have completed, within the last 7 years, at least 3 assignments of a similar nature and comparable complexity, being assignments involving the planning, design or implementation of intelligent transport systems, corridor modernisation, or comparable multi-agency technology programmes.

iii) Experience in Sub-Saharan Africa is not mandatory but is an advantage.

iv) Where the Consultant is a joint venture, these requirements shall be met by the joint venture taken as a whole, and the lead member shall itself meet the minimum of 10 years of experience and demonstrate at least 2 of the 3 required assignments.

v) The firm may sub-consult specialised areas of expertise, provided the arrangement is disclosed in the proposal.

vi) A firm, joint venture member, or sub-consultant participating in the selection of the Technical Advisor for the SMART Corridor Project shall not participate in the selection of the Design Consultant, whether as a firm, as a joint venture member, or as a sub-consultant, and the reverse shall apply equally. This restriction is necessary in order to preserve the independence of the Technical Advisor's review function.

12.2 Key and Non-Key Experts

The roles set out in Table 2 represent the minimum core competencies required. The Consultant may propose additional supporting experts or sub-consultants as needed, including for specialised areas such as UAV/drone systems, institutional reform, or other niche design requirements, provided that clear responsibility and coordination arrangements are demonstrated. Positions designated Key in Table 2 shall be proposed by name, supported by individual curricula vitae. Positions designated Non-Key shall be provided by the Consultant as part of the team and shall be reflected in the staffing schedule, but individual curricula vitae are not required. The person-months stated are minimum requirements; the Consultant shall propose the level of effort its methodology requires and shall justify any position proposed above the stated minimum. All Key and Non-Key Experts shall be proficient in written and spoken English, which is the working language of the assignment. Evaluation arrangements for each category shall be as set out in the Request for Proposals.

Table 2: Key and Non-Key Experts

#	Position	Qualification Requirements	Category	Minimum Person-Months
1	Team Leader / Senior ITS Expert	Master's degree in engineering, transport, or a related field At least 15 years of relevant professional experience with demonstrated involvement in projects related to transport systems, ITS, corridor management, or similar large-scale infrastructure or digital programmes Specific experience: demonstrated experience as Team Leader or Project Manager on at least 3 similar assignments in the past 10 years involving corridor development, intelligent transport systems, trade facilitation, or multi-agency transport infrastructure programmes.	Key	8
2	Systems Architect / Interoperability and Data Integration Lead	Master's degree in software engineering, ICT, or a related field At least 10 years of relevant professional experience in ITS systems architecture, digital platforms, or large-scale data systems Specific experience: at least 3 assignments in the past 10 years involving end-to-end ITS or multi-agency system architecture, including interoperability with existing government platforms.	Key	9
3	Enforcement, WIM, and Speed Camera Systems Specialist	Master's degree in engineering, ICT, transport, or a related field At least 10 years of relevant professional experience in enforcement, compliance, speed camera, ANPR, WIM, or related ITS-based control systems Specific experience: at least 3 assignments in the past 10 years involving automated enforcement, weigh-in-motion, or speed and ANPR back-office design, including	Key	7

#	Position	Qualification Requirements	Category	Minimum Person-Months
		evidential chain and adjudication workflows.		
4	Road / Civil / Pavement and Corridor Infrastructure Engineer	Bachelor's or Master's degree in civil or road engineering At least 10 years of relevant professional experience in road infrastructure, pavement, roadside installations, utilities coordination, bridge/culvert or structural works, or transport-corridor civil works Specific experience: at least 3 assignments in the past 10 years involving roadside ITS installation design, including foundations, ducting, power and communications routing within the road reserve.	Key	7
5	Trade Facilitation and OSBP Systems Expert	Master's degree in logistics, transport, ICT, customs/trade facilitation, or a related field At least 10 years of relevant professional experience in border operations, trade facilitation, OSBP processes, or digital freight / customs systems Specific experience: at least 3 assignments in the past 10 years involving One-Stop Border Post design, pre-arrival processing, risk management, or coordinated border management.	Key	5
6	Road Safety and Emergency Response Planning Specialist	Bachelor's or Master's degree in road safety, transport engineering, emergency planning, or a related field At least 8 years of relevant professional experience in road-safety engineering, blackspot analysis, post-crash response planning, or related corridor safety programmes Specific experience: at least 3 assignments in the past 8 years involving corridor road safety assessment, blackspot treatment, or post-	Key	5

#	Position	Qualification Requirements	Category	Minimum Person-Months
		crash and emergency response planning.		
7	Procurement and Tender Documentation Specialist	Bachelor's or Master's degree in engineering, procurement, law, quantity surveying, or a related field At least 10 years of relevant professional experience in the preparation of procurement and tender documentation for technology, infrastructure, or systems-integration contracts Specific experience: at least 3 assignments in the past 10 years involving preparation of procurement-ready tender documentation, technical specifications and employer's requirements for World Bank or comparably financed projects, including the packaging of works, goods, systems integration and services into separate contracts with defined interface responsibilities.	Key	6
8	Traffic Modelling and Transport Planning Expert	Master's degree in transport engineering, civil engineering, or a related field At least 10 years of relevant professional experience in traffic engineering, corridor analysis, transport planning, and mobility modelling Specific experience: at least 3 assignments in the past 10 years involving corridor or network traffic modelling, demand forecasting, and performance baseline development.	Non-Key	6
9	Business Analyst	Bachelor's or Master's degree in business analysis, information systems, engineering, or a related field At least 8 years of relevant professional experience in requirements engineering for complex, multi-stakeholder information systems	Non-Key	6

#	Position	Qualification Requirements	Category	Minimum Person-Months
		Specific experience: at least 3 assignments in the past 8 years involving requirements elicitation and specification for multi-agency or public sector digital systems, with demonstrated ability to convert business and operational needs into verifiable and testable system requirements.		
10	Cybersecurity, Data Governance, and Physical Security Specialist	Bachelor's or Master's degree in cybersecurity, ICT, engineering, or a related field At least 8 years of relevant professional experience in cybersecurity architecture, data governance, and protection of critical field infrastructure Specific experience: at least 3 assignments in the past 8 years involving cybersecurity and data governance design for government or critical infrastructure systems.	Non-Key	4
11	Digital Payments and Revenue Systems Specialist	Bachelor's or Master's degree in ICT, finance systems, engineering, or a related field At least 8 years of relevant professional experience in transport payments, electronic transactions, revenue systems, or public-sector payment integration Specific experience: at least 3 assignments in the past 8 years involving electronic payment, tolling, or revenue collection system design.	Non-Key	4
12	Legal, Institutional and Regulatory Specialist	Bachelor's or Master's degree in law, public administration, institutional development, or a related field At least 8 years of relevant professional experience in legal and regulatory review, institutional analysis, or in-	Non-Key	4

#	Position	Qualification Requirements	Category	Minimum Person-Months
		ter-agency governance arrangements in the transport, customs, or public infrastructure sectors Specific experience: at least 3 assignments in the past 8 years involving review of enabling legislation and regulatory frameworks, design of inter-agency governance or data-sharing arrangements, or institutional mapping for multi-agency public sector programmes.		
13	Telecommunications, Fibre and Connectivity Specialist	Bachelor's or Master's degree in telecommunications, electronic engineering, ICT, or a related field At least 8 years of relevant professional experience in fibre-optic and wide-area communications network assessment and design, including alternative and backup transmission technologies Specific experience: at least 3 assignments in the past 8 years involving assessment of existing fibre-optic infrastructure and design of connectivity, redundancy and quality-of-service arrangements for distributed field systems along transport corridors or comparable linear infrastructure.	Non-Key	4
14	Financial and O&M Cost Estimation Specialist	Bachelor's or Master's degree in economics, finance, quantity surveying, engineering economics, or a related field At least 8 years of relevant professional experience in capital and recurrent cost estimation, lifecycle costing, and operations and maintenance cost modelling for infrastructure or technology programmes Specific experience: at least 3 assignments in the past 8 years involving preparation of disaggregated CAPEX and OPEX estimates, recurrent-	Non-Key	4

#	Position	Qualification Requirements	Category	Minimum Person-Months
		cost sustainability analysis, and alternative implementation scenarios matched to different financing envelopes.		
	Total			**79**

13. Payment Schedule

Payments shall be tied to the satisfactory completion and formal acceptance of deliverables by the Employer.

Disbursements shall be made on a lump-sum basis per deliverable, in accordance with the agreed share of the total contract value allocated to each task, as presented in Table 3. The allocation reflects the expanded scope of services under these Terms of Reference, including integrated functional, technical and institutional design; corridor infrastructure and roadside facility considerations; trade facilitation and unified payment architecture; interoperability and data governance; cybersecurity and physical security; phased implementation planning; procurement packaging; and multi-agency consultations.

Cross-cutting stakeholder workshops, field validation activities, and limited on-the-job knowledge transfer shall be deemed included within the corresponding deliverables and shall not constitute a separate standalone payment item.

Release of the payment for Deliverable 4 shall additionally be conditional upon the Employer's acceptance of the procurement-ready tender package for Phase 1, prepared under Deliverable 5 and due at the end of Month 9.

Table 3: Allocation by Deliverable

Deliverable	Share of Total
D1 – Inception Report and Design Phase Work Plan	10%
D2 – Corridor Analysis and Baseline Assessment Report	17%
D3 – Functional, Technical and Institutional Design Report	28%
D4 – Phased Implementation Strategy and Cost Estimate	20%
D5 – Procurement Strategy and Tender Documentation for Implementation	15%
D6 – Final Design Consolidation and Handover Report	10%
Total	**100%**

14. Annex 1. System Design Principles

The requirements set out in this Annex are indicative. They describe the system as currently understood by the Employer and are provided to convey the scope, ambition, and operational outcomes sought. They are not a settled specification. The Consultant shall validate, refine, complete, and where justified depart from them, on the basis of the baseline assessment, stakeholder consultations, and the design work carried out under this assignment. Any departure shall be reasoned and documented in the relevant deliverable. The procurement-ready technical specifications prepared under Deliverable 5 shall supersede this Annex.

This Annex describes the system. It does not define the scope of funded deployment or the level of design detail required. Those are set out in the Scope of Work: funded scope differs by pillar, and site design is taken to concept level across it and to tender-ready level only for Phase 1. Nothing in this Annex extends either.

Contents of Annex 1

Contents of Annex 1 29
A1.1 Design Outcomes 29
A1.2 Overall System Architecture 30
A1.3 Functional Requirements 35
A1.4 Central Management and Analysis Software 56

A1.1 Design Outcomes

The design shall be capable of delivering the outcomes set out below. These are the outcomes sought from the implemented SMART Corridor system and are the reference against which the Consultant shall validate, refine and complete the indicative requirements in this Annex.

Safety. Reduced crash frequency and severity through proactive detection, early warning and coordinated response; improved speed compliance and driving behaviour; fewer secondary incidents through faster detection and clearance; protection of infrastructure through weigh-in-motion, load-condition and overheight detection; and a corridor safety programme linking analytics to blackspot treatment priorities, emergency-response workflows and practical roadside measures.

Corridor efficiency and reliability. Improved throughput and reduced delay at toll plazas, enforcement points and border crossings through risk-based, data-driven operation; improved travel-time reliability, particularly for freight and transit traffic; better coordination between tolling, enforcement and border processes; and faster recovery from incidents, peak demand and abnormal conditions.

Enforcement, compliance and security. More effective enforcement of speed, axle-load and vehicle compliance requirements; improved traceability of vehicle movements through integrated tolling, weigh-in-motion, ANPR, cargo tracking and electronic seal data; reduced reliance on manual roadside checks through automated, risk-based selection; and auditable, transparent enforcement processes.

Border and trade facilitation. Reduced border processing times through pre-arrival information, data sharing and risk management; support for non-stop or low-stop operation consistent with One-Stop Border Post principles; improved monitoring of freight movement and cargo integrity; enhanced coordination between border agencies through shared data and common operational visibility; and reduced transaction friction through aligned payment confirmation and document handling across agencies.

Corridor monitoring, performance and asset management. Corridor-wide visibility of traffic, freight and enforcement performance; reliable performance indicators including travel times, compliance rates and congestion patterns; the ability to identify bottlenecks, safety hotspots and operational inefficiencies; evidence-based monitoring to support operational and policy decisions; and visibility of pavement and roadside asset condition to support preventive maintenance planning.

Institutional coordination and long-term sustainability. Strengthened coordination between transport, enforcement, border and security institutions, with clear roles, data-sharing arrangements and defined governance of command, maintenance, data ownership and escalation; reduced fragmentation of systems and processes through interoperable platforms; high-quality historical data supporting long-term planning and before-and-after assessment; and a scalable architecture supporting corridor expansion, later integration with cooperative ITS services, and long-term protection of public investment through open, extensible design.

A1.2 Overall System Architecture

The Smart Traffic Corridor Management System shall be designed and implemented as a modular, scalable, resilient, and interoperable architecture, enabling real-time corridor operations, advanced analytics, and future system expansion. The architecture shall support high availability, cybersecurity, and seamless integration of heterogeneous ITS subsystems.

In addition, the system architecture shall support phased deployment through geographically and technically defined lots, segments, and technological modules. Each lot shall be capable of operating independently at the field, edge, and communication layers, while remaining fully interoperable with the central processing, data management, and application layers. This approach shall enable progressive implementation, prioritisation of high-impact locations and/or high-impact technological modules, and scalability over time without requiring architectural redesign.

For each lot, segment, and major activity area, the SMART Corridor system shall produce defined data types, interfaces, and outputs. These shall include, as applicable, traffic counts by vehicle class in accordance with the applicable national road classification system or as otherwise specified by the Employer, speeds, travel times, queue lengths, incidents, toll and payment events, WIM / axle-load data (integrated with existing RDA WIM systems), border-processing milestones, asset-status events, climate/flood alerts, imagery/video metadata, and the corresponding operational outputs such as dashboards, reports, evidence records, alerts, and KPI summaries.

The overall system architecture shall be structured into distinct but fully integrated layers, as described below.

A1.2.1 Architectural Principles

The system architecture shall be based on principles including, but not limited to, the following:

i) **Modularity:** Each subsystem shall operate as an independent module while remaining fully interoperable;

ii) **Scalability:** The architecture shall support corridor expansion, additional sensors, and increased data volumes without major redesign;

iii) **Open Standards:** Use of open, widely adopted protocols and interfaces to avoid vendor lock-in;

iv) **High Availability:** Redundant and fault-tolerant design for critical components;

v) **Cybersecurity-by-Design:** Security integrated at all architectural levels;

vi) **Real-Time Performance:** Low-latency data acquisition, processing, and visualization;

vii) **Future Readiness:** Compatibility with emerging ITS and C-ITS / V2X technologies.

A1.2.2 Field Layer (Sensing and Data Acquisition)

The Field Layer shall consist of all roadside and on-site equipment responsible for data collection and initial event detection.

Field devices shall include, but are not limited to:

i) Traffic scene analysis and incident detection cameras;

ii) Radar-based speed detection sensors and automated speed enforcement devices;

iii) ANPR cameras and illuminators;

iv) Weigh-in-Motion (WIM) systems;

v) Overheight vehicle detection sensors;

vi) Variable Message Signs (VMS);

vii) Toll collection equipment;

viii) Border gate security sensors and access control devices;

ix) Camera-based or automated monitoring for wash-aways, flood overtopping, drainage distress, culvert overtopping, and severe water-related pavement failures at high-risk crossing points that are hydrologically or geotechnically vulnerable;

x) Trade facilitation and border-support equipment, including queue detection devices, gate/lane control devices, e-seal readers, and interfaces to non-intrusive inspection systems where applicable;

xi) UAV/drone systems and associated station or docking infrastructure, where justified for corridor monitoring or post-crash management

Field Layer characteristics:

i) Continuous 24/7 operation;

ii) Day/night and all-weather capability;

iii) Time-stamped and geo-referenced data;

iv) Local preprocessing and edge analytics where applicable;

v) Physical protection measures for field assets, including tamper-resistant enclosures, secure mounting, power resilience, and health/tamper monitoring where appropriate.

A1.2.3 Edge Processing Layer

An Edge Processing Layer shall be deployed to enable low-latency decision making and reduce central system load.

Functions include:

i) Local AI inference for incident and violation detection;
ii) Data filtering, aggregation, and normalization;
iii) Temporary buffering in case of communication outages;
iv) Local health monitoring and diagnostics.

Edge components shall securely communicate with the central system and support remote configuration.

A1.2.4 Communication Layer

The Communication Layer shall provide secure and reliable data transmission between field devices, edge units, and central systems.

Communication technologies may include:

i) Fibre-optic networks, based on assessment of existing corridor fibre assets and, where necessary, provision for new fibre deployment or alternative communications infrastructure;
ii) LTE / 5G cellular communication;
iii) Microwave or wireless links (where applicable);
iv) Secure VPN tunnels with encryption and Quality of Service (QoS) for real-time data.

Requirements:

i) Redundant communication paths for critical locations;
ii) Quality of Service (QoS) for real-time data;
iii) Encrypted data transmission;
iv) Network monitoring and diagnostics.

A1.2.5 Central Processing and Data Management Layer

This layer shall host all central system components responsible for data storage, analytics, and orchestration.

Components include:

i) Application servers;
ii) AI and analytics engines;
iii) Databases (real-time, historical, and geospatial) forming a Central Data Repository;
iv) Integration and message brokers to facilitate multi-agency data exchange.

Functions:

i) Data fusion from multiple subsystems;
ii) Real-time event correlation;
iii) Historical data storage and retrieval;

iv) Analytics and KPI calculation;

v) Workflow and rule engine execution;

vi) Centralized orchestration of corridor-wide events and inter-agency alerts.

The system shall support horizontal and vertical scaling to accommodate future growth and shall be designed to prevent single-point failures in the data management architecture.

A1.2.6 Application and Management Layer

The Application Layer shall provide all user-facing functionalities.

Features include:

i) Central corridor operations dashboard (with agency-specific views for stakeholders such as RTSA, RDA, ZRA, and Police, providing access to relevant information based on mandate);

ii) GIS-based visualization of corridor assets, events, and climate-related alerts;

iii) Incident, enforcement, and environmental management modules;

iv) Management and visualization of a single clearing platform for tolls, fines, permit fees, and border-related charges;

v) VMS content management;

vi) User and role management aligned with institutional access rights;

vii) Reporting and analytics interfaces.

The user interface shall be web-based and accessible through standard browsers with support for secure mobile access where required.

A1.2.7 Integration and Interoperability Layer

The system shall include a dedicated integration layer to ensure seamless interoperability both among the different SMART Corridor functions/modules and with existing and future external systems.

Capabilities:

i) Open REST, MQTT, and HTTPS APIs;

ii) Data exchange with existing ITS, police, emergency, toll, and border systems (including the ZRA Electronic Cargo Tracking System and National Registration databases);

iii) Support for standardized data models where applicable;

iv) External data ingestion (e.g., national databases, weather services);

v) Shared use of field infrastructure, including poles, cabinets, power supply, communications, and mounting structures, where technically and operationally appropriate;

vi) Cross-module data exchange and event orchestration across CCTV/incident detection, ANPR, WIM, tolling, border, VMS, and central analytics functions;

vii) Common master data, time synchronisation, and event identifiers to support end-to-end corridor workflows and auditability.

A1.2.8 Cybersecurity Architecture

Cybersecurity shall be embedded across all architectural layers.

Measures include:

i) Secure authentication and authorization mechanisms;
ii) Role-based access control;
iii) Encrypted communication channels (End-to-End Encryption);
iv) System logging and audit trails to ensure legal admissibility of enforcement and financial records;
v) Intrusion detection and prevention mechanisms.

A1.2.9 High Availability and Disaster Recovery

The system architecture shall ensure continuous operation.

Requirements:

i) Redundant central system components;
ii) Failover mechanisms for critical services;
iii) Data backup and recovery procedures;
iv) Business continuity and disaster recovery planning, including manual fallback procedures for critical border and enforcement workflows.

A1.2.10 Deployment Models

The architecture shall support flexible deployment models and explicitly assess centralized, decentralized / distributed, and hybrid operating concepts.

i) Decentralized or hybrid deployment should be preferred where feasible in order to improve resilience, allow operational continuity by lot or agency, and reduce single-point dependencies;
ii) Possible deployment patterns include national on-premises data centers, regional or agency nodes, and government or private cloud services where permitted;
iii) The design shall clearly identify which functions, data, and services are best centralized (e.g., the Central Data Repository) and which should remain distributed or locally hosted (e.g., agency-specific operational platforms).

The chosen model shall be subject to Employer approval and comply with national data governance, cybersecurity regulations, and the TRACER project's environmental and social safeguards.

A1.2.11 Future Expansion and C-ITS Readiness

The architecture shall be designed to support future ITS developments, including:

i) Cooperative ITS (C-ITS) and V2X communication;
ii) Connected and autonomous vehicle integration;
iii) Advanced AI-driven predictive traffic management;
iv) Integration with digital twin platforms.

A1.3 Functional Requirements

The detailed requirement areas set out in the Functional Requirements and Central Management and Analysis Software parts of this Annex are indicative and non-exhaustive. They are intended to guide the Consultant's analysis and design work and shall not be interpreted as vendor-specific technical specifications or as limiting the Consultant's obligation to define fit-for-purpose performance requirements based on international ITS and corridor-management good practice.

A1.3.1 Camera-Based Incident Detection System (IDS)

The Smart Traffic Corridor shall include an advanced Camera-Based Incident Detection System (IDS) that utilizes AI-driven video analytics to automatically detect, classify, and report traffic incidents and abnormal traffic conditions in real time. The IDS shall serve as a core safety and operational component of the corridor, enabling proactive traffic management and rapid response.

A1.3.1.1 Functional Scope

The IDS shall continuously monitor traffic conditions and automatically detect incidents, including but not limited to:

i) Traffic accidents and collisions;
ii) Stopped or broken-down vehicles;
iii) Wrong-way driving;
iv) Sudden speed drops and shockwave formation;
v) Lane blockages and debris on roadway;
vi) Pedestrian or animal intrusion in restricted areas;
vii) Illegal stopping or parking on critical sections;
viii) Queue formation and spillback detection;
ix) Incidents occurring at high-risk "black spots" identified during the baseline assessment.

Detection shall be performed without operator intervention and shall function across all lanes and directions within the defined coverage areas.

A1.3.1.2 Detection Performance Requirements

i) Real-time detection with minimal latency;
ii) Configurable detection zones and Regions of Interest (ROI);
iii) Lane-level and direction-based analysis;
iv) High detection accuracy with defined and acceptable false-alarm rates appropriate to operational use;
v) Continuous operation under:
    a. Day and night conditions,
    b. Rain, fog, dust, and glare,
    c. Varying traffic densities.

The system shall allow performance tuning based on corridor-specific conditions.

Detection performance thresholds shall be measurable, testable, and verifiable during acceptance testing in accordance with international standards.

A1.3.1.3 AI and Video Analytics Capabilities

The IDS shall utilize modern AI and computer vision techniques, including but not limited to:

i) Object detection and tracking;
ii) Vehicle classification (car, truck, bus, motorcycle);
iii) Vehicle make/model recognition (where technically feasible and legally permitted);
iv) Vehicle counts per direction, lane, and turning movement, disaggregated by vehicle class;
v) Speed and trajectory analysis;
vi) Behavioural pattern recognition;
vii) Event correlation across multiple cameras.

The AI models shall support continuous improvement, re-training validation, and performance monitoring, subject to governance and approval procedures and data privacy protocols.

A1.3.1.4 Event Management and Alerting

Upon detection of an incident, the IDS shall:

i) Automatically generate a time-stamped and geo-referenced event;
ii) Classify the incident type and severity;
iii) Trigger real-time alerts to operators;
iv) Support automated actions such as:
    a. VMS message activation,
    b. Signal timing adjustment,
    c. Notification to emergency or maintenance teams and the Police command center.

Alerts shall be configurable based on incident type and priority.

A1.3.1.5 Integration with Corridor Subsystems

The IDS shall be fully integrated with the Smart Corridor Management Platform and other subsystems, including:

i) **Dynamic Intersection Management System (DIMS):** Adaptive signal response during incidents;
ii) **Variable Message Signs (VMS):** Automatic incident and safety messaging;
iii) **Radar Speed Detection and ANPR Systems:** Correlation of incidents with speed and vehicle data;
iv) **Traffic Analytics Modules:** Post-incident analysis and performance reporting.

A1.3.1.6 Video Management and Evidence Handling

The system shall provide integrated video management functions:

i) Live video streaming
ii) Event-based video recording
iii) Pre-event and post-event buffering
iv) Secure storage of video evidence
v) Video playback and export tools

Video data shall be protected against unauthorized access and tampering to ensure it meets legal evidentiary requirements.

A1.3.1.7 System Configuration and Operations

i) Centralized configuration of detection rules and thresholds;
ii) Remote health monitoring of cameras and analytics modules;
iii) Automatic fault and tamper detection;
iv) Support for maintenance and calibration procedures.

A1.3.1.8 Scalability and Expansion

i) Support for incremental addition of cameras and detection zones;
ii) Ability to extend detection capabilities to new incident types;
iii) Compatibility with future AI model upgrades.

A1.3.1.9 Compliance and Standards

The IDS shall comply with:

i) Relevant national road safety and ITS regulations;
ii) International ITS and video surveillance standards;
iii) Data protection and privacy regulations.

A1.3.1.10 Reporting and Performance Metrics

The system shall generate comprehensive reports, including:

i) Number and type of detected incidents;
ii) Detection and response times;
iii) False alarm rates;
iv) Incident locations and time-of-day analysis;
v) Before/after safety performance indicators.

A1.3.2 Dynamic Intersection Management System (DIMS)

The Smart Traffic Corridor shall include a Dynamic Intersection Management System (DIMS) designed to provide real-time, adaptive, and performance-driven control of signalized intersections along the corridor, particularly in urban areas, junctions near toll plazas, border approaches, and high-risk locations.

The system shall dynamically optimize signal operations using multi-source data fusion, advanced analytics, and rule-based and algorithmic decision mechanisms. DIMS shall operate both at local intersection level and corridor/network level, enabling coordinated traffic management under normal, congested, and incident conditions and shall specifically prioritize the reduction of delays at border approaches and weighbridge entries.

A1.3.2.1 Functional Scope

The DIMS shall support the following core functions:

i) Real-time traffic signal control and monitoring;
ii) Adaptive signal timing and phase optimization;

iii) Corridor-level coordination and green wave management;
iv) Priority handling for selected vehicle classes (including emergency response and authorized transit freight);
v) Scenario-based traffic management;
vi) Performance monitoring and optimization;
vii) Coordination with toll plaza and weighbridge approach management systems.

The system shall support both fully automatic operation and operator-assisted manual control.

A1.3.2.2 Data Inputs and Data Fusion

DIMS shall continuously ingest and process data from multiple sources, including:

i) Traffic volumes, queue length, and speed data from video analytics;
ii) Radar-based speed detection data;
iii) Vehicle trajectory and travel time data;
iv) Incident and abnormal traffic condition alerts;
v) Historical traffic and performance datasets;
vi) Real-time status of weighbridge queues and toll plaza saturation levels.

The system shall perform real-time data fusion to ensure robust decision-making under varying data quality and availability conditions.

Traffic flow optimization analyses shall include, where relevant, the development of WIM/weighbridge approach-area measures to reduce congestion, queue spillback, unsafe lane changes, and unnecessary stopping.

A1.3.2.3 Adaptive Signal Control Logic

The system may support limited adaptive control functions, such as:

i) Adjustment of cycle length and green splits;
ii) Time-of-day signal plans;
iii) Manual override by operators during incidents or congestion.

A1.3.2.4 Corridor Coordination and Green Wave Management (Optional)

Where justified by traffic conditions and corridor geometry, the system may support:

i) Dynamic green wave creation and adjustment;
ii) Direction-based prioritization;
iii) Time-of-day and demand-based coordination plans;
iv) Adaptive offset optimization.

Coordination strategies shall be automatically recalculated based on changing traffic conditions. These functions shall be considered optional and subject to feasibility assessment by the Design Consultant.

A1.3.2.5 Priority and Special Vehicle Handling

The system shall support conditional and dynamic priority for:

i) Emergency vehicles;
ii) Authorized and special-use vehicles.

Priority implementation shall remain simple and operationally manageable, aligned with institutional capacity and clear inter-agency protocols.

A1.3.2.6 Scenario-Based Traffic Management (Optional)

The DIMS may support predefined operational scenarios, such as:

i) Incident and accident response;
ii) Roadworks and lane closures;
iii) Severe weather events or flood-related diversions.

Scenarios may be automatically triggered or manually activated and shall include predefined signal strategies and operational rules.

A1.3.2.7 Performance Monitoring and KPI-Driven Optimization

The system shall continuously evaluate intersection and corridor performance using key performance indicators (KPIs), including:

i) Average delay per vehicle;
ii) Queue length and queue clearance time;
iii) Stop frequency;
iv) Throughput and saturation levels;
v) Level of Service (LoS) at critical corridor nodes.

Performance information shall be:

i) Aggregated at intersection and corridor levels;
ii) Visualised through operator dashboards within the central corridor management environment;
iii) Stored for historical analysis and comparison.

The system shall support:

i) Before/after analysis;
ii) Time-of-day and day-of-week comparisons;
iii) Strategy performance comparison.

A1.3.2.8 Historical Data Analysis and Reporting

The DIMS shall provide access to historical operational data for:

i) Trend analysis;
ii) Performance auditing;
iii) Policy evaluation;
iv) Optimization strategy refinement.

Reports shall be exportable and configurable.

A1.3.2.9 Compliance and Standards

The DIMS shall comply with:

i) National traffic signal and road safety regulations;
ii) International ITS standards;

iii) Cybersecurity and data protection requirements.

A1.3.3 Variable Message Sign (VMS) System

The Smart Traffic Corridor shall include a fully integrated Variable Message Sign (VMS) System designed to provide real-time, accurate, and context-aware information to road users. The VMS System shall function as a core communication and traffic guidance tool, supporting safety, efficiency, compliance, and user awareness across the corridor.

The system shall operate under centralized control, while supporting automatic, scenario-based, and operator-driven message generation.

A1.3.3.1 Functional Scope

The VMS System shall support the following functions:

i) Incident, accident, and hazard warnings;
ii) Speed and compliance feedback;
iii) Toll, border, and lane status messaging;
iv) Emergency and special event announcements.

Messages shall be dynamically updated based on real-time corridor conditions.

A1.3.3.2 Message Types and Content Management

The system shall support:

i) Text- and symbol-based messages compliant with national road-traffic signage and communication regulations;
ii) Dynamic message updates based on real-time corridor information;
iii) Centralised activation and deactivation of messages.

Message content shall be managed through the central corridor management environment, ensuring consistency and operational control.

A1.3.3.3 Integration with Traffic Management Systems

The VMS System shall be fully integrated with other corridor subsystems, including:

i) **Dynamic Intersection Management System (DIMS):** Support adaptive strategies by influencing driver behaviour;
ii) **Incident Detection System (IDS):** Automatic warning and diversion messages;
iii) **Radar Speed Detection and ANPR Systems:** Speed feedback and compliance messaging;
iv) **Weigh-in-Motion (WIM) Systems:** Advance notification to drivers approaching weigh-in-motion locations, compliance messaging related to axle load and loading conditions;
v) **Overheight Detection System:** Immediate warning and diversion instructions;
vi) **Toll and Border Systems:** Queue status, lane availability, and advisory messages.

Predefined message libraries aligned with incident, enforcement, weather, toll, and border-operation scenarios

A1.3.3.4 Operator Interface and Manual Control

The system shall provide operators with:

i) Real-time status view of all VMS units;
ii) Manual message composition and deployment;
iii) Scenario selection and override capability;
iv) Message preview and approval workflow;
v) User role-based permissions.

All operator actions shall be logged and auditable to ensure transparency in corridor management.

A1.3.3.5 Performance Monitoring and Effectiveness Analysis

The VMS System shall include analytics to assess message effectiveness, including:

i) Message activation frequency and duration;
ii) Correlation with traffic flow and speed changes;
iii) Compliance impact (e.g., speed reduction after message display);
iv) Before/after analysis for safety and congestion scenarios.

These analytics shall support continuous improvement of messaging strategies.

A1.3.3.6 Technical and Operational Requirements

i) Compliance with national and international VMS standards;
ii) High visibility and legibility under all lighting conditions, including configurable brightness and contrast adjustment based on ambient conditions.

The design shall also assess where VMS should be complemented by improved fixed road signage, delineation, or high-retroreflectivity warning and regulatory signs so that driver guidance remains effective under day, night, adverse-weather, and power-outage conditions.

i) Support remote monitoring and basic fault diagnostics;
ii) Redundant power and communication where required (e.g., solar power with battery backup for remote corridor sections to ensure 24/7 availability);
iii) Secure communication and access control;
iv) Design for incremental expansion as corridor ITS functions evolve.

A1.3.4 Vehicle Tracking System (VTS)

The Smart Traffic Corridor shall include a comprehensive Vehicle Tracking System (VTS) designed to provide real-time and historical visibility of vehicle movements along the corridor. The VTS shall support operational traffic management, performance analysis, enforcement support, trade facilitation, and strategic planning through continuous tracking and analytics.

The system shall function as a data fusion and visualization layer, aggregating vehicle movement information from multiple sensing technologies.

A1.3.4.1 Functional Scope

The VTS shall support the following core functions:

i) Real-time tracking of vehicle movements along the corridor;

ii) Visualization of vehicle trajectories on a GIS-based map;
iii) Monitoring of vehicle speed, direction, and travel time;
iv) Detection of abnormal or non-compliant vehicle behaviour;
v) Support for enforcement, tolling, and border operations;
vi) Historical analysis of corridor usage and performance;
vii) Monitoring of transit times for trade facilitation to identify administrative or physical bottlenecks.

A1.3.4.2 Data Sources and Tracking Methods

The VTS shall integrate and correlate data from multiple sources, including but not limited to:

i) Automatic Number Plate Recognition (ANPR) systems;
ii) Radar-based speed detection sensors;
iii) Video analytics-based vehicle tracking;
iv) Toll collection systems;
v) Weigh-in-Motion (WIM) and enforcement systems;
vi) Border gate and access control systems;
vii) Electronic Cargo Tracking Systems (ECTS) and electronic seals, where applied to transit freight;
viii) Optional external data sources (e.g., authorized GPS feeds or fleet-management feeds), subject to legal approval.

The system shall reconcile data from different sources to generate continuous and reliable vehicle trajectories, even when individual data streams are intermittent.

A1.3.4.3 Real-Time Tracking and Visualization

The system shall provide:

i) Real-time and near-real-time visualization of vehicle movements on corridor maps;
ii) Direction-based and lane-aware tracking where available;
iii) Configurable filters by vehicle class, speed, or freight status;
iv) Event overlays (incidents, congestion, enforcement actions, or border delays).

Visualization shall support both individual vehicle views (where legally permitted) and aggregated traffic flow representations.

A1.3.4.4 Travel Time and Corridor Performance Analysis

The VTS shall automatically compute:

i) Section-based and corridor-wide travel times;
ii) Average, minimum, and maximum travel speeds;
iii) Traffic volumes and traffic counts by vehicle class, direction, and selected section, using the applicable national road classification system or such classification scheme as the Employer may specify;
iv) Travel time reliability and variability indicators;
v) Bottleneck and delay location identification.

These metrics shall be available in real time and for historical analysis.

A1.3.4.5 Behavioural and Compliance Analysis

The system shall support the detection and analysis of:

i) Identification of abnormal routing or unexplained delays;
ii) Detection of inconsistencies between toll, WIM, border, and ECTS data;
iii) Support to enforcement and security agencies for risk-based follow-up.

The system shall focus on exception detection, rather than continuous behaviour profiling.

A1.3.4.6 Integration with Corridor Systems

The VTS shall be fully integrated with other corridor subsystems, including:

i) **Dynamic Intersection Management System (DIMS):** Demand estimation and adaptive control support;
ii) **Incident Detection System (IDS):** Incident verification and trajectory analysis;
iii) **Radar Speed Detection and ANPR Systems:** Speed enforcement and compliance correlation;
iv) **Variable Message Sign (VMS) System:** Travel time and advisory messaging;
v) **Toll, WIM, and Border Gate Systems:** Throughput and queue monitoring.

A1.3.4.7 Alerts and Operational Support

The system shall generate alerts based on configurable conditions, including:

i) Abnormally slow or stopped vehicles;
ii) Unexpected route deviations;
iii) Excessive travel times;
iv) Repeated non-compliance events.

Alerts shall be prioritized and routed to operators through the central platform and shared with relevant agency command centres based on established protocols.

A1.3.4.8 Historical Data Analysis and Reporting

The VTS shall provide extensive reporting capabilities, including:

i) Origin-destination (OD) flow analysis;
ii) Time-of-day and day-of-week traffic patterns;
iii) Corridor usage trends by vehicle class;
iv) Freight movement and transit performance indicators;
v) Enforcement and compliance performance indicators.

Reports shall be configurable, exportable, and suitable for decision-making and planning.

A1.3.4.9 Data Privacy and Legal Compliance

The VTS shall be designed in compliance with:

i) National data protection and privacy regulations;
ii) Role-based access controls and data minimization principles;
iii) Clear rules on data ownership, access rights, and permitted use.

Personally identifiable data shall be accessed only by authorized users and only for legally permitted purposes.

A1.3.4.10 Scalability and Future Readiness

The VTS shall be capable of:

i) Scaling to additional corridor segments and regions;
ii) Integrating future data sources as they become available;
iii) Supporting predictive and AI-based traffic modeling.

A1.3.5 Integrated Radar and Automatic Number Plate Recognition System (Speed & Compliance Monitoring)

The Smart Traffic Corridor shall include an Integrated Radar and Automatic Number Plate Recognition (ANPR) System designed to provide accurate, reliable, and continuous monitoring of vehicle speed, identity, and compliance. The system shall support real-time traffic management, automated enforcement workflows, toll and border operations, and strategic traffic analysis.

Radar sensors and ANPR cameras shall operate as tightly coupled but modular components, enabling both instantaneous and average speed measurement, while ensuring legally traceable vehicle identification.

A1.3.5.1 Functional Scope

The integrated system shall support the following core functions:

i) Instantaneous speed measurement (point speed);
ii) Average speed measurement (section control);
iii) Multi-lane and bi-directional monitoring;
iv) Automatic license plate recognition;
v) Vehicle identification and classification;
vi) Detection of speed and compliance violations;
vii) Support for tolling, border, and access control operations.

A1.3.5.2 Radar-Based Speed Detection Capabilities

Radar sensors shall provide:

i) Non-intrusive, contactless speed measurement;
ii) Multi-target tracking in dense traffic;
iii) Lane-level speed detection;
iv) High accuracy at urban and highway speeds;
v) Configurable speed thresholds aligned with road class, posted limits, and regulatory enforcement rules;
vi) Reliable operation under all weather and lighting conditions (e.g., heavy rain, dust, and glare typical of the corridor environment).

Radar data shall include:

i) Vehicle speed;
ii) Lane and direction;

iii) Time and location;

iv) Detection confidence level.

A1.3.5.3 Automatic Number Plate Recognition Capabilities

The ANPR component shall provide:

i) High-accuracy plate recognition across multiple national and regional plate formats, including future formats;

ii) Recognition at varying vehicle speeds;

iii) Day/night and adverse weather operation;

iv) Vehicle attribute extraction, including:

   a. Vehicle type,

   b. Colour,

   c. Make/model (where feasible);

v) High-resolution image capture of the vehicle and driver (where technically feasible) for evidentiary purposes.

Each ANPR event shall be:

i) Time-stamped;

ii) Geo-referenced;

iii) Associated with radar speed data when applicable.

A1.3.5.4 Integrated Speed Enforcement and Compliance Workflows

The system shall support automated enforcement use cases, including:

i) Point speed enforcement;

ii) Average speed (section control) enforcement;

iii) Speed compliance monitoring without enforcement;

iv) Restricted lane and access violation detection;

v) Toll and border compliance verification.

For enforcement-oriented use cases, the system shall generate evidence packages, including:

i) Radar-measured speed;

ii) Applicable speed limit;

iii) License plate data;

iv) Vehicle images;

v) Time, date, and location;

vi) Confidence indicators and certification of the radar unit's calibration status.

A1.3.5.5 Real-Time Alerts and Watchlist Matching

The system shall support real-time matching against configurable lists, including:

i) Speed thresholds aligned with road class, posted limits, and applicable enforcement rules;

ii) Blacklists and hotlists (e.g., stolen vehicles or vehicles with unpaid fines);

iii) Authorized and exempt vehicle lists.

Matches shall trigger role-based and priority-based actions, including:

i) Operator alerts;
ii) Integration actions (e.g., VMS messaging, access control);
iii) Secure event logging and notification handling.

Operator alerts prioritised according to risk level, watchlist type, and operational context

A1.3.5.6 Integration with Corridor Subsystems

The integrated Radar + ANPR system shall be fully interoperable with:

i) **Vehicle Tracking System (VTS):** Construction of vehicle trajectories and travel time analysis;
ii) **Dynamic Intersection Management System (DIMS):** Speed-aware adaptive signal strategies;
iii) **Incident Detection System (IDS):** Correlation of abnormal speed patterns with incidents;
iv) **Variable Message Sign (VMS) System:** Speed feedback, compliance warnings, and safety messages;
v) **Automatic Toll Collection, WIM, and Border Systems:** Vehicle identification, compliance, and throughput analysis.

A1.3.5.7 Data Management and Storage

The system shall provide:

i) Secure storage of radar and ANPR events;
ii) Configurable data retention and anonymization policies;
iii) Fast search and retrieval by plate, time, location, or violation type;
iv) Export of authorized datasets for reporting and analysis.

All records shall be protected against unauthorized access and tampering.

A1.3.5.8 Operator Interface and Review Tools

The system shall provide operators with:

i) Real-time event visualization;
ii) Image and speed review tools;
iii) Manual verification and correction capabilities;
iv) Full audit trails for all actions.

Access shall be controlled through role-based permissions.

A1.3.5.9 Data Protection and Legal Compliance

The system shall comply with:

i) National data protection and privacy regulations;
ii) Legal evidentiary requirements for enforcement use cases;
iii) Data minimization and access control principles.

Personally identifiable information shall only be accessible to authorized users.

A1.3.5.10 Scalability and Future Readiness

The integrated system shall be designed to:

i) Scale to additional corridor segments and entry points;
ii) Support new plate formats and jurisdictions;
iii) Integrate with national enforcement and vehicle databases;
iv) Support future C-ITS / V2X-based speed and compliance services.

A1.3.5.11 Performance Metrics and Reporting

The system shall provide measurable outputs, including:

i) Speed compliance rates;
ii) Violation detection accuracy;
iii) Average and percentile speed statistics;
iv) Enforcement processing times;
v) System availability, reliability, and response-time metrics for event detection and alert generation.

A1.3.6 Automatic Toll Collection System (ATCS)

The SMART Corridor design shall assess and, where justified, define the technical concept, road-side infrastructure, communications, and back-office provisions required to enable future implementation of an Automatic Toll Collection System (ATCS) and/or e-tolling functions. The Government may elect not to implement e-tolling under the present phase; however, the design shall make future deployment materially easier and shall ensure interoperability with other corridor functions.

The design shall examine how toll operations and future tolling infrastructure interact with traffic flow, including queue monitoring, lane management, VMS integration, and congestion-reduction measures at toll approaches.

A1.3.6.1 Functional Scope

The ATCS shall support the following core functions:

i) Automatic vehicle identification for tolling purposes;
ii) Free-flow toll collection without the need for physical barriers;
iii) Support for multiple tolling technologies;
iv) Toll transaction recording, validation, and reconciliation;
v) Violation detection and compliance monitoring;
vi) Centralized toll operations management.

A1.3.6.2 Vehicle Identification and Tolling Methods

The system shall support one or more of the following identification methods:

i) Automatic Number Plate Recognition (ANPR);
ii) Electronic tags or transponders (where applicable);
iii) Hybrid identification combining ANPR and tag data.

The system shall reliably associate vehicle identity with toll events at varying speeds and traffic densities.

A1.3.6.3 Toll Transaction Processing

The ATCS shall:

i) Accurately record toll transactions in real time;
ii) Apply configurable toll pricing rules based on:
    a. Vehicle class,
    b. Time of day,
    c. Corridor segment,
    d. Special conditions or policies;
iii) Support centralized transaction validation and reconciliation;
iv) Support for prepaid, postpaid, and account-based tolling models, where required by the selected implementation and commercial framework;
v) Provide secure storage of all transaction records.

A1.3.6.4 Violation Detection and Enforcement Support

The system shall detect and record toll violations, including:

i) Non-payment events;
ii) Incorrect vehicle classification;
iii) Unauthorized lane usage.

For each violation, the system shall generate a verifiable event record, including:

i) Vehicle identification;
ii) Time and location;
iii) Toll amount and violation type;
iv) Supporting image and sensor data.

A1.3.6.5 Integration with Corridor Subsystems

The ATCS shall be fully integrated with:

i) **Integrated Radar and ANPR System:** Vehicle identification and compliance verification;
ii) **Vehicle Tracking System (VTS):** Toll zone entry and exit validation;
iii) **Variable Message Sign (VMS) System:** Toll information, pricing, and lane availability messages;
iv) **Border Gate and Access Control Systems:** Cross-border toll compliance and throughput management;
v) **Central Corridor Management Platform:** Unified operations and reporting.

A1.3.6.6 Operator Interface and Management Tools

The system shall provide operators with:

i) Real-time monitoring of toll operations;
ii) Transaction and violation review tools;

iii) Manual verification and correction workflows;
iv) Pricing rule configuration interfaces;
v) Role-based access control.

All operator actions shall be logged and auditable.

A1.3.6.7 Revenue Management and Analytics

The ATCS shall include advanced analytics, including:

i) Toll revenue reporting;
ii) Traffic volume and revenue correlation;
iii) Peak and off-peak usage analysis;
iv) Violation statistics and recovery rates;
v) Performance indicators for toll operations.

Reports shall be configurable and exportable.

A1.3.6.8 Data Management and Security

i) Secure storage of toll transaction data;
ii) Encrypted data transmission;
iii) Configurable data retention and anonymization;
iv) Compliance with financial and data protection regulations.

A1.3.6.9 Reliability, Availability, and Continuity

i) High-availability system design;
ii) Redundant processing and communication paths;
iii) Automated fault detection and alerting;
iv) Fail-safe operating modes to prevent unsafe conditions or material traffic disruption during partial system outages;
v) Business continuity and recovery procedures.

A1.3.6.10 Compliance and Standards

The ATCS shall comply with:

i) National tolling and transportation regulations;
ii) Financial transaction security standards;
iii) Data protection and privacy laws.

A1.3.6.11 Scalability and Future Readiness

The system shall be designed to:

i) Support expansion to additional toll zones;
ii) Enable dynamic pricing and policy changes;
iii) Integrate with national toll and payment platforms and support alignment with a broader multi-agency corridor payment ecosystem;
iv) Interface with permit payments, penalties, weighbridge-related fees, border charges, payment confirmation, reconciliation, and reporting;

v) Support future mobility and pricing models.

A1.3.6.12 Performance Metrics and Outputs

The system shall provide measurable outputs, including:

i) Transaction accuracy rate;
ii) Violation detection rate;
iii) Revenue collection efficiency;
iv) System uptime and availability.

A1.3.7 Border and One-Stop Border Post (OSBP) Digital System

The SMART Corridor design shall define the required Border and One-Stop Border Post (OSBP) digital interfaces and operating concepts needed to support efficient, coordinated, and risk-based border operations, while improving throughput, compliance, and transparency at linked corridor border gateways and control interfaces, as applicable.

The Border and OSBP Digital System shall complement existing platforms, including the Electronic Cargo Tracking System (ECTS) implemented under ZATP-II, and shall form an integral component of the broader SMART Corridor architecture.

The design shall also define a broader corridor trade facilitation architecture, including workflow mapping, data-exchange logic, and institutional interfaces for customs, border agencies, freight-control processes, ECTS, e-seals, smart gates / smart yards, tolling, WIM, permits, inspections, and payment-confirmation processes, so that border digitalisation is embedded within an end-to-end transit operating model.

A1.3.7.1 Functional Scope

The Border and OSBP Digital System shall support the following core functions:

i) Automated vehicle and freight identification at border entry and exit points;
ii) Digital support to OSBP operations through coordinated workflows among border agencies;
iii) Support to non-stop or low-stop border operations through pre-arrival processing and selective controls;
iv) Collection, validation, and sharing of border-related information prior to arrival;
v) Monitoring of queues, waiting times, and border throughput.

The design shall specify the trade facilitation-related systems and equipment required, including, but not limited to:

i) Border gate ANPR/camera equipment;
ii) Smart gate and smart yard interfaces;
iii) Queue and lane monitoring devices;
iv) E-seal readers;
v) Workstation and inspection-support interfaces;
vi) Gate/lane control devices;
vii) Traveller or operator submission interfaces;

viii) Integration points for scanners or other non-intrusive inspection technologies, where applicable;

ix) Support to risk-based inspections and enforcement actions;

x) Integration with corridor-wide monitoring, tracking, and enforcement systems.

A1.3.7.2 Definition of Required Documents and Information

This activity shall include:

i) Mapping of documents and data currently required by each border agency;

ii) Identification of redundancies, overlaps, and opportunities for harmonisation under OSBP arrangements;

iii) Definition of a minimum common data set required for border processing;

iv) Alignment with national legislation, existing systems, and applicable bilateral / OSBP arrangements;

v) Preparation of a consolidated document and data requirements matrix to guide system design.

A1.3.7.3 Online Pre-Arrival Information System

The system shall include an online pre-arrival information module allowing transport operators or agents to submit required information before reaching the border.

The pre-arrival system shall support:

i) Structured online forms aligned with the defined document and data requirements;

ii) Submission of vehicle, cargo, and trip information prior to arrival;

iii) Upload of supporting documents where required;

iv) Automated checks for completeness and consistency;

v) Controlled access for border agencies to review information in advance;

vi) Integration with existing customs and trade platforms (e.g., ASYCUDA World) to ensure that required declarations are validated prior to arrival at the border;

vii) Support for digital tokens or automated identifiers to enable fast-track processing at Smart Gates for pre-cleared vehicles.

This module shall support coordinated OSBP processing, enabling agencies to prepare inspections and decisions prior to vehicle arrival, thereby reducing on-site processing time and ensuring that physical inspections are only conducted on a risk-justified basis.

A1.3.7.4 Risk Analysis and Risk-Based Border Processing

The Border and OSBP Digital System shall support risk analysis and profiling to enable targeted and efficient border controls.

Risk-based functions shall include:

i) Use of pre-arrival data, historical records, and corridor monitoring data to assess risk levels;

ii) Identification of high-risk vehicles, consignments, or trips;

iii) Detection of inconsistencies between declared information and observed corridor data;

iv) Support to selective inspections rather than blanket controls;

v) Automated "Routing Logic" that assigns vehicles to specific inspection lanes (Green/Yellow/Red) based on the risk score.

Risk indicators and alerts shall be accessible to relevant agencies through the central platform and dashboards.

A1.3.7.5 Vehicle Identification and Border Event Recording

The system shall support automated identification and recording of border crossing events through:

i) Capture of vehicle images at border entry and exit points;

ii) Automatic Number Plate Recognition (ANPR), where applicable;

iii) Time-stamped and geo-referenced recording of border transactions.

Border event data shall be linked to pre-arrival submissions and corridor monitoring records.

A1.3.7.6 Electronic Seal (E-Seal) Integration

The Border and OSBP Digital System shall support integration with electronic cargo seal (e-seal) systems used for transit monitoring and with associated smart gate / smart yard workflows where applicable.

E-seal integration shall include:

i) Association of e-seal identifiers with vehicles, containers, and border transactions;

ii) Monitoring of seal status (intact, tampered, broken);

iii) Detection of route deviations or abnormal stops where e-seal data is available;

iv) Interoperability with ECTS, smart gate / smart yard functions, and corridor tracking systems.

E-seal data shall contribute to risk analysis and enforcement support without duplicating ZRA-led systems but rather by enriching the corridor-wide visibility.

A1.3.7.7 Queue, Throughput, and Operational Monitoring

The system shall support monitoring of border operations, including:

i) Real-time queue length and waiting time monitoring;

ii) Throughput statistics by vehicle and cargo type;

iii) Monitoring of queue spillback, gate-processing bottlenecks, and upstream/down-stream impacts on wider corridor operations;

iv) Peak period and congestion analysis;

v) Performance indicators for border operations;

vi) Automated broadcasting of estimated border wait-times to upstream VMS units and the Corridor Mobile App to allow for proactive driver rest-stop planning.

A1.3.7.8 Integration with Corridor Systems

The Border and OSBP Digital System shall be fully integrated with:

i) The Central Data Repository and Corridor Monitoring Platform;

ii) Vehicle Tracking System (VTS);

iii) Automatic Toll Collection System (ATCS);

iv) Weigh-in-Motion System (WIM);

v) Variable Message Sign (VMS) System;

vi) Coordinated border management platforms and existing customs systems (e.g., ASYCUDA World) to ensure a unified data entry point for all participating agencies.

The design shall specify the API (Application Programming Interface) requirements to ensure that data from WIM and ANPR units can be used to automatically validate border declarations in real-time.

A1.3.7.9 User Access, Dashboards, and Data Governance

The system shall provide role-based access and tailored dashboards for participating agencies, allowing:

i) Real-time visibility of border operations relevant to each mandate;

ii) Access to risk indicators, alerts, and performance metrics;

iii) Audit trails and activity logging.

Data access shall comply with national data protection and governance requirements.

A1.3.7.10 Scalability and Future Readiness

The Border and OSBP Digital System shall be designed to:

i) Support expansion to additional lanes and checkpoints;

ii) Adapt to evolving OSBP procedures and regulatory frameworks;

iii) Integrate additional data sources and technologies over time;

iv) Support future enhancements in digital trade facilitation and risk management.

A1.3.8 Weigh-in-Motion (WIM), Vehicle Profile, and Overheight Vehicle Detection System (OHDS)

The SMART Corridor shall include an integrated Weigh-in-Motion (WIM), Vehicle Profile, and Overheight Vehicle Detection System (OHDS), designed to support infrastructure protection, regulatory compliance, and corridor safety through non-intrusive, in-motion monitoring of heavy vehicles.

The system shall enable the detection of:

i) Vehicles exceeding predefined height clearance thresholds;

ii) Vehicles exceeding weight and axle-load thresholds;

iii) Abnormal vehicle loading configurations that may pose safety or infrastructure risks.

The system shall support preventive and risk-based actions, without requiring vehicles to stop, and shall contribute to low-stop corridor operations to minimize fuel consumption and greenhouse gas emissions associated with heavy vehicle idling.

A1.3.8.1 Functional Scope

The integrated WIM, Vehicle Profile, and OHDS shall support the following core functions:

i) Detection of vehicles exceeding a predefined height threshold;

ii) Measurement of gross vehicle weight and axle loads using WIM technology;

iii) Analysis of vehicle profile and loading configuration, including abnormal height, shape, or load distribution.

The design shall also define supplier-neutral integration requirements for existing weighbridges, WIM stations, and related back-office systems, including interface standards, data mapping, event identifiers, communications requirements, and interoperability rules so that equipment and software originating from different suppliers can be integrated into the SMART Corridor environment without avoidable duplication or vendor lock-in.

i) Lane-specific and direction-based detection;
ii) Early warning generation upstream of height- or weight-restricted infrastructure;
iii) Event logging, monitoring, and data sharing with corridor systems;
iv) Support for preventive safety, compliance screening, and selective enforcement.

A1.3.8.2 Detection Principles and Technologies

The system shall operate using a combination of threshold-based detection and classification logic, including:

i) Overheight detection (binary threshold: below/above clearance);
ii) Weigh-in-motion measurement of gross vehicle weight, axle loads, axle configuration;
iii) Vehicle profile analysis to identify abnormal load height, irregular load shape or protrusions, unsafe load distribution;

The system may utilize one or a combination of the following technologies:

i) WIM sensors embedded in the pavement;
ii) Optical beam or infrared beam interruption systems;
iii) Laser curtain or light barrier systems;
iv) Vision-based detection with fixed reference thresholds;
v) Hybrid sensor configurations for redundancy and validation.

Key characteristics:

i) No requirement for vehicles to stop;
ii) Configurable clearance threshold by location and infrastructure type;
iii) Reliable operation under day/night and adverse weather conditions;
iv) Detection at operational traffic speeds.

A1.3.8.3 Real-Time Alerts and Warning Mechanisms

Upon detection of a non-compliant vehicle (overheight, overweight, or abnormal vehicle profile), the system shall:

i) Generate an immediate time-stamped and geo-referenced event;
ii) Trigger automated warning mechanisms, including:
    a. Variable Message Sign (VMS) alerts,
    b. Visual warning signals (e.g. flashing lights),
    c. Audible warnings where applicable,
    d. Operator notifications in the control centre.

Alert logic shall be configurable and prioritized.

A1.3.8.4 Integration with Corridor Systems

The WIM, Vehicle Profile, and OHDS shall be fully integrated with:

i) Variable Message Sign (VMS) System: Display of warnings and diversion guidance;
ii) Dynamic Intersection Management System (DIMS): Support for speed reduction or diversion strategies;
iii) Electronic Cargo Tracking System (ECTS) and e-Seal systems: Correlation between physical vehicle characteristics and declared cargo data;
iv) Incident Detection System (IDS): Correlation with near-miss or strike incidents;
v) Vehicle Tracking and ANPR Systems: Identification and tracking of non-compliant vehicles;
vi) Central Corridor Management Platform: Unified monitoring, alerting, and reporting.

A1.3.8.5 Support to Preventive and Risk-Based Actions

The system shall support predefined preventive and risk-based corridor management actions, including:

i) Early diversion guidance for non-compliant vehicles;
ii) Advance warnings before toll plazas;
iii) Risk-based selection of vehicles for further checks at downstream control points;
iv) Reduction of infrastructure damage and unsafe movements.

A1.3.8.6 Event Recording and Evidence Management

For each detected event, the system shall store:

i) Detection status (overheight, overweight, abnormal vehicle profile);
ii) Measured weight and axle-load parameters (WIM);
iii) Associated image(s) or video snapshot(s), where available;
iv) Time, date, and detection location;
v) Triggered warning and response actions.

All records shall be securely stored and retrievable for analysis and reporting.

A1.3.8.7 Analytics and Performance Evaluation

The system shall provide analytical tools to support:

i) Identification of recurring non-compliance patterns;
ii) Assessment of infrastructure risk exposure;
iii) Evaluation of preventive warning effectiveness;
iv) Support to planning of enforcement locations and infrastructure upgrades.

A1.3.8.8 Reliability, Availability, and Maintenance

i) Continuous 24/7 operation;
ii) Sensor redundancy where required;
iii) Automatic fault detection and alerts;
iv) Remote diagnostics and maintenance support.

A1.3.8.9 Compliance and Standards

The system shall comply with:

i) National road safety, axle-load, and infrastructure protection regulations;
ii) Relevant ITS and safety standards;
iii) Cybersecurity and data protection requirements.

A1.3.8.10 Scalability and Future Readiness

The system shall be designed to:

i) Support additional monitoring locations;
ii) Allow threshold reconfiguration based on infrastructure changes;
iii) Integrate with future connected vehicle warning services;
iv) Support predictive safety analytics.

A1.3.8.11 Performance Metrics and Outputs

The system shall provide measurable outputs, including:

i) Overweight and over height detection accuracy;
ii) False detection rate;
iii) Warning activation response time;
iv) Reduction in infrastructure strike incidents;
v) System uptime and availability.

A1.4 Central Management and Analysis Software

The SMART Corridor shall include a fully integrated, web-based Central Management and Analysis Software Platform that serves as the common analytical, monitoring, and decision-intelligence environment for all corridor subsystems.

The platform shall act as the central data aggregation, visualization, and analytical layer, enabling participating institutions to access real-time and historical corridor information through role-based dashboards, while allowing each agency to retain responsibility for its own operational systems.

The platform shall support:

i) Real-time corridor monitoring and situational awareness;
ii) Performance analysis and reporting;
iii) Evidence-based decision support for enforcement, safety, trade facilitation, and corridor management;
iv) Controlled data sharing among institutions in line with defined governance arrangements;
v) Corridor asset management.

The design shall clearly define the concept for a central corridor data repository and control point, including the designated data custodian/system host, the relationship between the central platform and agency-operated systems, and the rules for real-time, near-real-time, and historical data access by participating institutions.

A1.4.1 General Software Architecture

The Central Management and Analysis Software shall be designed using a modern, modular, interoperable, and scalable software architecture that enables integrated corridor operations and advanced analytics, while ensuring long-term sustainability, maintainability, and interoperability.

A web-based, browser-accessible architecture is preferred, allowing authorized users to access the system through standard web browsers. Any use of additional client-side components shall be limited, optional, and technically justified.

A1.4.1.1 Architectural Principles

The software architecture shall adhere to the following core principles:

i) **Modularity:** Functional components shall be implemented as independent modules or services, enabling incremental deployment, simplified maintenance, and future expansion;

ii) **Microservice-Based Design:** The system shall use a microservice-based or similarly modular architecture that allows independent scaling, updating, and controlled evolution of individual services;

iii) **Geographical Segmentation and Lot-Based Deployment:** The architecture shall explicitly support geographical segmentation of the corridor into independent but interoperable lots or sections, allowing phased implementation by location or priority area. Each geographical lot shall be manageable independently while remaining fully integrated into the central data and management environment;

iv) **Scalability:** The architecture shall support scaling from a single-corridor deployment to multi-corridor, city-wide, or national-level systems without major redesign;

v) **Interoperability:** Open interfaces and standardized communication mechanisms shall be used to ensure seamless integration with external ITS, enforcement, security, and smart city platforms;

vi) **Vendor Neutrality and Licensing:** Licensing and technology choices shall favour open standards and open interfaces; where proprietary software is proposed, the base system should, wherever practicable, be supplied with perpetual or otherwise durable licences and clearly defined rights for continued Government operation;

vii) **High Availability and Resilience:** The architecture shall support redundancy, failover mechanisms, and graceful degradation to ensure continuous operation of critical services.

A1.4.1.2 Web-Based User Access and Interface Layer

i) User access shall be provided through a web-based, browser-accessible interface, compatible with commonly used modern web browsers;

ii) The user interface shall be responsive and support different screen sizes and resolutions;

iii) No mandatory desktop software installation shall be required for standard operator, analyst, or supervisory functions;

iv) Role-based user interfaces shall be supported, presenting relevant tools, data, and controls according to user authorization levels.

A1.4.1.3 Application and Business Logic Layer

The application layer shall host all core system functionalities, including:

i) Traffic and corridor management logic;
ii) Incident, enforcement, and compliance workflows;
iii) AI-assisted analytics and decision-support functions;
iv) Scenario management and operational rule engines;
v) Reporting, KPI computation, and visualization services.

Business logic shall be centrally managed to ensure consistency across all subsystems and operational views.

A1.4.1.4 Data Management and Storage Layer

The system shall include a robust data management layer supporting:

i) Real-time data ingestion from field systems and external sources;
ii) Historical data storage for long-term analysis and auditing;
iii) Geospatial data management for 2D and 3D visualization;
iv) High-volume event, transaction, and log data storage.

The architecture shall support the use of multiple database technologies (e.g., relational, time-series, geospatial, object storage) where appropriate.

A1.4.1.5 Analytics and AI Processing Layer

The architecture shall include dedicated components for:

i) Real-time analytics and multi-source event correlation;
ii) Historical and big-data analytics;
iii) Execution of AI models for prediction, anomaly detection, and optimization;
iv) Monitoring of analytics and AI model performance.

AI processing may be performed centrally and/or at edge locations, depending on latency and operational requirements.

A1.4.1.6 Integration and API Layer

The system shall expose a comprehensive integration layer, including:

i) Open REST / HTTPS APIs;
ii) Event-driven or message-based interfaces;
iii) Secure data exchange mechanisms for third-party systems.

All APIs shall be documented and designed to support interoperability and avoid vendor lock-in.

A1.4.1.7 Security Architecture

Security shall be embedded across all architectural layers, including:

i) Secure authentication and authorization mechanisms;
ii) Role-based access control;
iii) Encrypted data transmission and storage;
iv) System logging, monitoring, and full audit trails.

The architecture shall comply with applicable national and international cybersecurity and data protection requirements.

A1.4.1.8 Deployment, Maintainability, and Lifecycle Management

The software architecture shall support flexible deployment and long-term operation, including:

i) Deployment in on-premises, cloud, or hybrid environments;
ii) Compliance with national data sovereignty and security policies;
iii) Remote software updates, patching, and configuration management;
iv) Configuration version control and rollback mechanisms;
v) Centralized system health monitoring and diagnostics;
vi) Long-term maintainability and extensibility of the platform.

A1.4.2 Unified Subsystem Integration

The platform shall provide central aggregation, monitoring, and analytics for all corridor subsystems, including:

i) Camera-Based Incident Detection and Video Analytics;
ii) Dynamic Intersection and Corridor Management;
iii) Variable Message Sign (VMS) System;
iv) Vehicle Tracking and Travel Time Analysis;
v) Integrated Radar + ANPR Speed & Compliance Monitoring;
vi) Automatic Toll Collection;
vii) Border and OSBP System;
viii) WIM and Overheight Vehicle Detection.

All subsystems shall share common data models, visualization layers and analytics engines. User administration shall be role-based and federated, so that each agency retains administration of access to its own operational systems while the platform manages access to central data and analytics.

A1.4.3 Web-Based Operational Dashboards (2D & 3D)

The Central Management and Analysis Software shall provide integrated, web-based operational dashboards supporting both 2D and 3D geospatial visualization, enabling operators, supervisors, and decision-makers to maintain real-time situational awareness of corridor operations.

The dashboards shall be designed to support multiple, agency-specific dashboards, each tailored to the operational mandate, responsibilities, and data access rights of the participating institution. The platform shall serve as the "Front-End" for the Corridor Digital Twin, allowing for the simulation of traffic impacts before physical interventions are made.

A1.4.3.1 Agency-Specific and Configurable Dashboards

Each participating agency shall be provided with a dedicated, configurable dashboard, allowing:

i) Access only to data relevant to the agency's legal mandate and operational role;
ii) Visualization of corridor information through customized views, indicators, and map layers;
iii) Configuration of widgets, charts, alerts, and KPIs according to operational needs;
iv) Role-based differentiation between operational, supervisory, and decision-making users.

Dashboards shall be configurable without software redevelopment, enabling agencies to adapt views over time as operational needs evolve.

A1.4.3.2 2D and 3D Geospatial Visualization

The dashboards shall support:

i) 2D map-based visualization of the corridor, road network, and assets using standard GIS layers (e.g., ArcGIS or OpenStreetMap compatible);

ii) 3D visualization of the corridor environment, including:

   a. Road geometry and intersections,

   b. Bridges, tunnels, gantries, and elevation changes,

   c. Traffic control and sensing assets (signals, VMS, cameras, sensors).

Users shall be able to seamlessly switch between 2D and 3D views within the same web interface.

A1.4.3.3 Real-Time Operational Overlays

The dashboards shall provide real-time visualization layers, including:

i) Traffic flow, speed, and congestion levels;

ii) Queue formation and spillback indicators;

iii) Incident, enforcement, toll, and border events;

iv) Environmental and meteorological conditions;

v) System health and asset status.

Visualization layers shall be toggleable and configurable by user role. The system shall support "Time-Slider" functionality, allowing supervisors to "play back" the map overlays to a specific point in time for incident post-mortem analysis.

A1.4.3.4 Asset and Event Interaction

The dashboards shall allow users to:

i) Select and inspect corridor assets and events directly from the map;

ii) View contextual information, status, and historical data;

iii) Access related video, images, or event records where applicable;

iv) Navigate between related events and subsystems;

v) Initiate direct actions from the dashboard, such as pushing a manual message to a specific VMS or clearing a false-alarm incident.

This interaction shall support rapid operational assessment and response while maintaining a full audit log of which operator accessed which data or triggered which command.

A1.4.3.5 Time-Based Visualization and Playback

The system shall support time-aware visualization, enabling users to:

i) Replay historical traffic, incident, and enforcement conditions;

ii) Analyse before/after scenarios;

iii) Observe temporal evolution of congestion, incidents, or environmental conditions;

iv) Synchronize playback of map data with recorded CCTV/Video feeds to provide a complete "360-degree" reconstruction of corridor incidents.

Time controls shall be available within both 2D and 3D views. The playback module shall include "Watermarking" and "Hash-Verification" to ensure that exported historical data is tamper-proof for use in legal proceedings or insurance claims.

A1.4.3.6 Dashboard Customization and User Profiles

The dashboards shall support:

i) Role-based layouts and data visibility;

ii) User-configurable widgets and map layers;

iii) Saving and recalling custom dashboard configurations.

This shall allow different operational units to work efficiently within the same platform.

A1.4.3.7 Performance and Usability Requirements

i) Dashboards shall be responsive and usable on standard desktop displays;

ii) Rendering performance shall support real-time updates without disrupting operations;

iii) The interface shall be intuitive and suitable for continuous 24/7 operation.

A1.4.3.8 Integration with Decision Support and Scenarios

The dashboards shall integrate with:

i) AI-assisted recommendations and alerts;

ii) Scenario management and operational workflows;

iii) KPI visualization and performance monitoring.

This integration shall support informed and coordinated decision-making.

A1.4.4 AI-Driven Traffic Intelligence and Decision Support

The Central Management and Analysis Software shall include an AI-driven traffic intelligence and decision-support layer that continuously analyses real-time and historical corridor data to support proactive, data-informed operational decisions.

The AI layer shall function as an operator-assistance system, providing actionable insights and recommendations, while ensuring that final operational control remains with authorized personnel. The AI system shall specifically support the "Contingent Emergency Response Component (CERC)" by providing the data triggers and impact simulations required to activate and manage emergency corridor protocols.

A1.4.4.1 Data-Driven Situational Awareness

The AI-driven layer shall continuously process data from multiple subsystems, including traffic sensors, video analytics, enforcement systems, environmental sensors, and historical databases, in order to:

i) Detect emerging congestion and abnormal traffic patterns using predictive algorithms that identify "bottleneck formation" before a total standstill occurs;

ii) Identify potential safety risks and incident precursors (e.g., detecting "secondary accident" risks when a primary incident has already slowed traffic);

iii) Recognize deviations from expected corridor performance (e.g., identifying when a vehicle's travel time between two points significantly exceeds the historical average, suggesting an unreported breakdown or unauthorized stop);

iv) Provide early warning indicators to operators.

This capability shall enhance situational awareness beyond simple threshold-based alerts.

A1.4.4.2 Predictive and Proactive Insights

The system shall provide predictive insights, including:

i) Short-term forecasts of traffic demand and congestion levels;

ii) Anticipation of queue spillback and bottleneck formation;

iii) Prediction of incident likelihood under prevailing conditions;

iv) Identification of periods with elevated operational risk.

Predictions shall be updated continuously as new data becomes available.

A1.4.4.3 Decision-Support Recommendations

Based on its analysis, the AI layer shall generate context-aware recommendations, such as:

i) Suggested signal timing or corridor coordination adjustments;

ii) Recommended VMS messages and placement strategies;

iii) Proposed speed management or diversion measures;

iv) Incident mitigation and recovery actions.

Recommendations shall be presented clearly, with supporting context, and shall be reviewable and controllable by operators.

A1.4.4.4 Learning from Historical Performance

The AI-driven system shall utilize historical data to:

i) Identify recurring congestion and safety patterns;

ii) Assess the effectiveness of past operational strategies;

iii) Support continuous refinement of recommendations;

iv) Enable comparison of similar situations across time.

This learning capability shall contribute to ongoing improvement of corridor operations.

A1.4.4.5 Explainability and Operator Trust

To support operator confidence and accountability, the system shall:

i) Provide high-level explanations for AI-generated alerts and recommendations;

ii) Reference key input factors (e.g. traffic volume, incidents, weather);

iii) Allow operators to understand why a recommendation was generated;

iv) Provide a "Confidence Score" for each AI-generated insight (e.g., "90% confidence that this is a vehicle breakdown"), allowing operators to prioritize higher-certainty events.

The system shall avoid "black-box" behaviour in operational decision-support functions.

A1.4.4.6 Integration with Operational Workflows

AI-driven insights and recommendations shall be fully integrated into:

i) Operational dashboards (2D and 3D views);
ii) Scenario management and response workflows;
iii) KPI monitoring and performance evaluation modules.

This integration shall ensure that AI intelligence is delivered at the point of decision-making, not as a separate or disconnected tool.

A1.4.4.7 Monitoring and Continuous Improvement

The system shall support:

i) Monitoring of AI recommendation usage and outcomes;
ii) Feedback mechanisms based on operator actions;
iii) Periodic performance evaluation of AI-assisted decisions.

These capabilities shall enable continuous improvement of AI effectiveness while maintaining operational transparency.

A1.4.5 AI-Assisted Dynamic Traffic Management

The Central Management and Analysis Software shall include AI-assisted dynamic traffic management capabilities that support the continuous optimization of corridor and intersection operations under varying demand, incident, and environmental conditions.

The AI functionality shall operate as a decision-support mechanism, assisting operators with timely, data-driven recommendations, while ensuring that final control authority remains with authorized personnel.

A1.4.5.1 AI-Supported Traffic Control Optimization

The system shall analyse real-time and historical data to support AI-assisted optimization of:

i) Signal timing parameters and phase allocation;
ii) Corridor coordination and progression strategies;
iii) Speed management and compliance measures;
iv) Traffic flow distribution during peak and off-peak periods.

Recommendations shall adapt dynamically to changing traffic conditions.

A1.4.5.2 Incident-Aware and Context-Sensitive Control

The AI-assisted system shall consider contextual factors such as:

i) Detected incidents and lane blockages;
ii) Congestion severity and queue spillback risk;
iii) Weather and environmental conditions;
iv) Special events, roadworks, or border/toll congestion;
v) Real-time capacity of diversion routes before recommending a traffic shift, ensuring that diversions do not create secondary bottlenecks.

Based on these factors, the system shall propose control strategies aimed at maintaining safety, minimizing disruption, and accelerating recovery.

A1.4.5.3 Corridor-Level and Network-Aware Management

AI-assisted control shall operate beyond isolated intersections, supporting:

i) Corridor-level traffic flow balancing;
ii) Direction-based prioritization during directional peaks;
iii) Prevention of secondary congestion propagation;
iv) Coordinated responses across multiple intersections and assets.

This shall enable a holistic, network-aware management approach.

A1.4.5.4 Human-in-the-Loop Control and Overrides

The system shall support a human-in-the-loop operating model, ensuring that:

i) AI-generated recommendations are presented for operator review;
ii) Operators can accept, modify, or reject recommendations;
iii) Manual overrides can be applied at any time;
iv) All actions and decisions are logged for audit and evaluation.

This approach shall preserve accountability and operational control.

A1.4.5.5 Learning and Continuous Improvement

The AI-assisted system shall learn from operational outcomes by:

i) Comparing recommended actions with actual results;
ii) Identifying strategies that yield consistent improvements;
iii) Refining future recommendations based on historical performance.

Learning mechanisms shall be transparent and aligned with operational policies.

A1.4.5.6 Integration with Operational Scenarios and KPIs

AI-assisted dynamic traffic management shall be integrated with:

i) Scenario management and operational workflows;
ii) Performance KPI monitoring and evaluation;
iii) Before/after analysis of implemented strategies.

This integration shall support evidence-based decision-making and continuous performance optimization.

A1.4.6 Big-Data Analytics and Historical Intelligence

The Central Management and Analysis Software shall include a big-data analytics and historical intelligence layer capable of processing, storing, and analysing large volumes of heterogeneous corridor data generated by traffic management, enforcement, environmental, and security subsystems.

This capability shall support both real-time operational insight and long-term strategic analysis, enabling data-driven evaluation, planning, and continuous improvement of corridor performance.

A1.4.6.1 Multi-Source Data Ingestion and Processing

The system shall support high-volume data ingestion from multiple sources, including:

i) Traffic sensors, cameras, and video analytics;
ii) Signal controllers and corridor control systems;
iii) Radar, ANPR, toll, and border security systems;

iv) Environmental and meteorological sensors;

v) System logs, events, and operational metadata.

Data ingestion shall support streaming and batch processing to accommodate both real-time and historical use cases.

A1.4.6.2 Scalable Data Storage and Management

The analytics platform shall provide scalable data storage supporting:

i) Short-term, high-frequency operational data;

ii) Long-term historical datasets for trend analysis;

iii) Geospatial and time-series data;

iv) Event, transaction, and enforcement records.

Data storage shall be optimized for fast querying, aggregation, and retrieval.

A1.4.6.3 Historical Trend and Pattern Analysis

The system shall enable historical analysis to:

i) Identify recurring congestion and safety patterns;

ii) Analyse seasonal, weekly, and daily traffic variations;

iii) Detect long-term changes in corridor usage and demand;

iv) Evaluate the impact of infrastructure or policy changes.

These insights shall support evidence-based planning and investment decisions.

A1.4.6.4 Comparative and Before/After Analysis

The platform shall support comparative analytics, including:

i) Before/after evaluation of implemented traffic strategies;

ii) Comparison across different time periods, locations, or scenarios;

iii) Assessment of operational performance under varying conditions.

Comparative analysis shall be supported through configurable dashboards and reports.

A1.4.6.5 Integration with AI and Decision Support

Historical and big-data analytics shall feed into:

i) AI-driven prediction and anomaly detection models;

ii) Performance benchmarking and KPI evaluation;

iii) Scenario analysis and decision-support workflows.

This integration shall ensure that AI-assisted recommendations are grounded in historical evidence.

A1.4.6.6 Data Quality, Consistency, and Validation

The system shall include mechanisms for:

i) Monitoring data completeness and consistency;

ii) Identifying anomalies, gaps, or sensor malfunctions;

iii) Supporting data validation and cleansing processes.

Maintaining high data quality shall be essential for reliable analytics and decision-making.

A1.4.6.7 Reporting and Knowledge Extraction

The analytics layer shall support:

i) Generation of historical performance reports;
ii) Extraction of insights for policy and operational reviews;
iii) Visualization of long-term trends using charts, maps, and timelines.

Reports shall be configurable and exportable for internal and external use.

A1.4.6.8 Support for Strategic Planning and Evaluation

Big-data analytics shall support strategic use cases, including:

i) Corridor capacity and demand forecasting;
ii) Safety and risk assessment over extended periods;
iii) Evaluation of sustainability and environmental objectives;
iv) Support for funding, reporting, and regulatory requirements.

A1.4.7 Traffic Performance and KPI Management

The Central Management and Analysis Software shall include a traffic performance and KPI management module that continuously monitors, evaluates, and visualizes the operational performance of the corridor and its subsystems.

The module shall support objective, data-driven performance assessment for operational control, reporting, and continuous improvement.

A1.4.7.1 KPI Definition and Calculation

The system shall support calculation and management of key performance indicators (KPIs), including but not limited to:

i) Traffic volumes, speeds, and travel times;
ii) Queue length, delay, and stop frequency;
iii) Level of Service (LOS) indicators;
iv) Incident frequency and response times;
v) Speed, toll, and access compliance indicators.

KPIs shall be configurable by location, time period, and operational scenario.

A1.4.7.2 Visualization and Monitoring

KPIs shall be visualized through:

i) Dashboards and charts;
ii) Map-based and corridor-level views;
iii) Time-based trend displays.

Visualization shall support both real-time monitoring and historical review.

A1.4.7.3 Comparative and Performance Evaluation

The system shall support:

i) Before/after comparison of traffic strategies;

ii) Performance comparison across time periods and locations;

iii) Integration of KPI results into scenario evaluation and reporting.

This capability shall support evidence-based decision-making and performance optimization.

A1.4.8 Integrated Enforcement and ANPR Back-Office

The Central Management and Analysis Software shall include a fully integrated, web-based enforcement and ANPR back-office module that supports end-to-end management of compliance, enforcement, and review workflows across the corridor.

The module shall be designed to support operational efficiency, legal traceability, and auditability, while ensuring compliance with applicable data protection regulations.

The allocation of case ownership, review authority, and enforcement decision-making between institutions is not settled by this Annex. It shall be defined under the institutional, legal and governance work set out in the Scope of Work, and the module shall be designed to support the allocation agreed.

A1.4.8.1 Centralized Event and Violation Management

The system shall provide centralized management of enforcement-related events, including:

i) Speed and compliance violations;

ii) Toll and access violations;

iii) Border and security-related events;

iv) Overheight detection events (where applicable).

All events shall be time-stamped, geo-referenced, and linked to supporting evidence.

A1.4.8.2 Evidence Review and Validation

The back-office shall provide tools for:

i) Review of images, video, and sensor data;

ii) Verification and validation of ANPR results;

iii) Manual confirmation or correction where legally permitted;

iv) Packaging of evidence records for downstream processes.

All review actions shall be logged for audit purposes.

A1.4.8.3 Search, Filtering, and Case Handling

The system shall support advanced search and filtering by:

i) License plate or vehicle identifier;

ii) Container ID (where applicable);

iii) Time, location, or event type;

iv) Enforcement or compliance status.

The module shall support grouping and handling of related events as part of structured workflows.

A1.4.8.4 Watchlists and Authorization Management

The system shall support:

i) Management of blacklists, whitelists, and watchlists;
ii) Real-time matching and alert generation;
iii) Controlled access to sensitive lists based on user roles.

A1.4.8.5 Integration and Traceability

The enforcement back-office shall be fully integrated with:

i) Radar and ANPR detection systems;
ii) Vehicle tracking and corridor analytics;
iii) Toll and border systems;
iv) Central reporting and KPI modules.

End-to-end traceability from detection to review and reporting shall be ensured.

A1.4.9 Vehicle Movement, OD, and Corridor Analytics

The Central Management and Analysis Software shall include a vehicle movement, origin–destination (OD), and corridor analytics module that provides insight into how vehicles use the corridor over time, supporting both operational management and strategic planning.

The module shall leverage data from multiple subsystems to produce aggregated, privacy-compliant mobility intelligence.

A1.4.9.1 Vehicle Trajectory and Movement Analysis

The system shall support:

i) Reconstruction of vehicle movements along the corridor;
ii) Analysis of speed profiles and travel behaviour;
iii) Identification of recurring movement patterns and anomalies;
iv) Aggregation of vehicle trajectories into flow-based representations.

Analysis shall be available in both real-time and historical contexts.

A1.4.9.2 Origin–Destination (OD) Analysis

The module shall enable OD analysis by:

i) Estimating entry and exit points along the corridor;
ii) Aggregating OD flows by time period and vehicle class;
iii) Supporting comparative analysis across different days, periods, or scenarios.

OD results shall support traffic planning, demand management, and policy evaluation.

A1.4.9.3 Corridor Performance and Bottleneck Identification

The system shall support analytics to:

i) Identify recurrent bottlenecks and delay locations;
ii) Evaluate corridor usage intensity and imbalance;
iii) Detect changes in routing behaviour over time.

These insights shall support targeted operational and infrastructure interventions.

A1.4.9.4 Visualization and Reporting

Vehicle movement and OD analytics shall be visualized through:

i) Map-based flow diagrams (2D and 3D where applicable);
ii) Charts and summary tables;
iii) Time-based trend views.

Results shall be available through dashboards and exportable reports.

A1.4.9.5 Integration with Other Analytics and KPIs

The module shall integrate with:

i) Traffic performance and KPI management;
ii) AI-driven traffic intelligence and decision support;
iii) Scenario evaluation and historical analysis.

This integration shall enable comprehensive, corridor-wide mobility assessment.

A1.4.10 Environmental and Sustainability Intelligence

The system shall support:

i) Real-time visualization of air quality and meteorological conditions;
ii) Spatial identification of environmental hotspots along the corridor;
iii) Overlay of environmental indicators with traffic and incident data.

Visualization shall be available through dashboards and map-based views.

A1.4.10.1 Correlation and Impact Analysis

The module shall enable:

i) Correlation of traffic conditions with environmental indicators;
ii) Identification of operational patterns contributing to environmental impact;
iii) Support for evaluation of emission-aware traffic strategies.

A1.4.10.2 Reporting and Sustainability Support

The system shall provide:

i) Historical environmental trend reports;
ii) Support for sustainability and Environmental, Social, and Governance (ESG)-related reporting;
iii) Data inputs for policy and planning assessments.

A1.4.11 Scenario Management and Digital Twin-Style Operations

The Central Management and Analysis Software shall include a scenario management and digital twin–style operational module that supports planning, simulation, and coordinated response for a wide range of traffic and corridor conditions.

This capability shall enable operators and decision-makers to prepare for, respond to, and evaluate both routine and exceptional operational scenarios.

A1.4.11.1 Scenario Definition and Activation

The system shall support the definition and management of scenarios, including:

i) Peak-hour congestion scenarios;
ii) Traffic incidents and lane closures;
iii) Adverse weather and environmental conditions;
iv) Special events and abnormal demand patterns;
v) Border, toll, or infrastructure-related disruptions.

Scenarios may be activated manually or automatically based on real-time conditions.

A1.4.11.2 Digital Twin–Style Visualization

The module shall support:

i) Visualization of scenarios on 2D and 3D corridor models;
ii) Representation of traffic flow, incidents, and control actions;
iii) Layer-based comparison of different operational states.

This visualization shall support shared situational awareness across operational teams.

A1.4.11.3 Scenario Evaluation and Comparison

The system shall enable:

i) Comparison of alternative response strategies;
ii) Visualization of expected and observed impacts using KPIs;
iii) Before/after analysis of scenario outcomes.

This capability shall support evidence-based selection of operational strategies.

A1.4.11.4 Integration with AI and Operational Workflows

Scenario management shall be integrated with:

i) AI-driven traffic intelligence and recommendations;
ii) Dynamic traffic management and control workflows;
iii) KPI monitoring and reporting modules.

This integration shall ensure that scenarios are directly actionable within daily operations.

A1.4.11.5 Post-Scenario Review and Learning

The system shall support:

i) Post-event review and replay of scenarios;
ii) Evaluation of response effectiveness;
iii) Capture of lessons learned for future operations.

This capability shall support continuous operational improvement.

A1.4.12 Reporting, Visualization, and Data Export

The software shall provide comprehensive reporting capabilities, including:

i) Customizable reports and dashboards;
ii) Interactive charts, maps, and 3D visualizations;

iii) Export in standard formats (PDF, CSV, XLSX, JSON);

iv) Scheduled and automated report generation.

A1.4.13 User, Role, and Audit Management

The platform shall support:

i) Role-based access control;

ii) Multi-level authorization;

iii) Secure authentication;

iv) Full audit logging of user and AI-driven actions.

A1.4.14 Integration, APIs, and Interoperability

The Central Management and Analysis Software shall provide a comprehensive integration and interoperability framework to enable secure and reliable data exchange with internal subsystems and external platforms.

The integration framework shall support open standards, extensibility, and long-term interoperability.

The integration framework shall also define licensing, interface-access, and data-exchange assumptions so that future subsystem procurement can proceed without undue proprietary dependency.

A1.4.14.1 API and Interface Support

The system shall provide:

i) Open, documented REST / HTTPS APIs;

ii) Event-based or message-driven interfaces where required;

iii) Secure authentication and authorization for API access.

APIs shall support both real-time data exchange and historical data retrieval.

A1.4.14.2 External System Integration

The platform shall support integration with:

i) Existing ITS and traffic management systems;

ii) Enforcement, police, emergency, and border systems;

iii) Smart city, mobility, transport-observatory, and data platforms.

Integration shall be designed to avoid vendor lock-in, support multi-vendor subsystem integration, and facilitate future extensions.

A1.4.14.3 Data Models and Interoperability

The system shall use:

i) Consistent and extensible data models;

ii) Standardized identifiers for assets and events;

iii) Clearly defined data ownership and exchange rules.

This approach shall ensure sustainable interoperability across systems and organizations.

A1.4.15 Security, Availability, and Deployment

The platform shall support:

i) End-to-end cybersecurity measures;
ii) High-availability and failover configurations;
iii) On-premises, cloud, or hybrid deployment;
iv) Centralized system health and performance monitoring;
v) Security-by-design measures across field devices, communications, applications, databases, and user interfaces;
vi) Network segmentation, identity and access management, secure remote administration, and least-privilege controls;
vii) Vulnerability management, patching procedures, security logging, monitoring, incident response, and recovery arrangements;
viii) Physical hardening and tamper-resistance requirements for roadside and field assets;
ix) Data retention, archival, and deletion policies aligned with legal, regulatory, and operational requirements;
x) On-premises, cloud, or hybrid deployment, with due regard to the preferred decentralized/hybrid operating model and to cybersecurity obligations;
xi) Centralized system health, performance, and security monitoring.

A1.4.16 Future Readiness and AI Evolution

The software shall be designed to:

i) Support future C-ITS / V2X integration;
ii) Enable continuous AI model evolution;
iii) Integrate with simulation and digital twin platforms;
iv) Adapt to evolving traffic, enforcement, and sustainability policies.

A1.4.17 Performance Metrics and Outputs

The platform shall provide measurable outputs, including:

i) System response time and latency;
ii) AI recommendation accuracy and utilization;
iii) Data completeness and quality;
iv) User engagement and system usage metrics.

15. Annex 2. Glossary of Terms and Abbreviations

The glossary set out in Table 4 is indicative and shall be refined and expanded by the Consultant during the assignment as necessary.

Table 4: Glossary of Terms and Abbreviations

Term / Abbreviation	Meaning
SMART Corridor	"Safety, Mobility, Automated, Real-time Traffic Management" Corridor: Integrated corridor concept combining digital, physical, and operational

Term / Abbreviation	Meaning
	measures to improve corridor performance, safety, enforcement, and trade facilitation
ITS	Intelligent Transport Systems
VRU	Vulnerable Road User
ANPR	Automatic Number Plate Recognition
WIM	Weigh-In-Motion
OHDS	Overheight Detection System
VMS	Variable Message Sign
OSBP	One-Stop Border Post
ECTS	Electronic Cargo Tracking System
UAV / Drone	Unmanned Aerial Vehicle
API	Application Programming Interface
SLA	Service Level Agreement
ConOps	Concept of Operations