



# **Request for Proposal (RFP) for Design, Development, Deployment and Maintenance of Unified NHAI ATMS Software**

## **VOLUME 2: SCOPE OF WORK AND REQUIREMENTS SPECIFICATIONS**

**RFP No.: IHMCL/Unified NHAI ATMS SW/2026/01**

**Date: 26 May 2026**



**Table of Contents**

<b>1. KPI Achievement Framework .....</b>	<b>12</b>
<b>1.1. Preamble.....</b>	<b>12</b>
<b>1.2. Platform Design Intent .....</b>	<b>12</b>
<b>1.3. SDA's Scope Boundary in Achieving KPIs .....</b>	<b>13</b>
1.3.1. SDA Responsibility.....	13
1.3.2. SDA – Out of Scope.....	14
<b>1.4. Module-to-KPI Responsibility Mapss .....</b>	<b>14</b>
<b>1.5. KPI / Outcome Expectations — SDA Platform Delivery Obligations .....</b>	<b>16</b>
<b>1.6. KPI Measurement, Reporting, and Review — SDA's Platform Obligations.....</b>	<b>23</b>
1.6.1. Real-Time KPI Visibility (Continuous — Platform Uptime).....	23
1.6.2. Daily Automated Reports (Module 5 — Pre-Built Report Library).....	23
1.6.3. Monthly KPI Review Package .....	24
1.6.4. Quarterly Audit Data Package .....	24
<b>1.7. Platform Replication and SOP for New Corridors.....</b>	<b>24</b>
<b>1.8. Summary: The Commitment to Outcome-Oriented Platform Design .....</b>	<b>24</b>
<b>2. Broad Scope of Work of Software Development Agency (SDA) .....</b>	<b>26</b>
<b>3. Programme Overview and Strategic Context .....</b>	<b>29</b>
<b>3.1. Programme Objectives .....</b>	<b>29</b>
<b>3.2. Scope of This Document .....</b>	<b>30</b>
<b>3.3. Architectural Mandate — Three-Tier Command Structure.....</b>	<b>30</b>
<b>3.4. Technical Network Architecture .....</b>	<b>32</b>
<b>3.5. Work Package Structure .....</b>	<b>33</b>
<b>3.6. 1,200 KM CORRIDOR DEPLOYMENT — RESPONSIBILITIES &amp; WORKFLOW .....</b>	<b>34</b>
3.6.1. Infrastructure Already In Place — What the SDA Inherits .....	34
3.6.2. The Three Principal Stakeholders — Roles and Authorities .....	35
3.6.3. Step-by-Step Deployment Walkthrough — 6 Stages.....	37
3.6.4. Consolidated Responsibility Matrix .....	40
<b>4. NATIONAL ATMS OPERATIONAL CONCEPT .....</b>	<b>43</b>
<b>4.1. System Purpose and Vision .....</b>	<b>43</b>
<b>4.2. Key Stakeholders .....</b>	<b>43</b>
<b>4.3. Operational Scenarios .....</b>	<b>44</b>
4.3.1. Normal Operations .....	44
4.3.2. Incident Response Operations .....	45

4.3.3.	Enforcement Operations .....	45
4.3.4.	Severe Weather and Disaster Operations.....	45
4.3.5.	Cyber Incident Response.....	45
<b>5.</b>	<b>NATIONAL – REGIONAL – LOCAL COMMAND AND CONTROL CENTRE HIERARCHY .....</b>	<b>47</b>
<b>5.1.</b>	<b>National Command and Control Centre (NCCC) .....</b>	<b>47</b>
5.1.1.	NCCC Functional Responsibilities .....	47
<b>5.2.</b>	<b>Regional Command and control Centres (RCCC) .....</b>	<b>48</b>
<b>5.3.</b>	<b>Local Command and Control Centres (LCCC) .....</b>	<b>49</b>
<b>5.4.</b>	<b>Operational Architecture .....</b>	<b>50</b>
<b>5.5.</b>	<b>Incident Monitoring Authority Matrix .....</b>	<b>51</b>
<b>6.</b>	<b>OVERALL SYSTEM ARCHITECTURE .....</b>	<b>52</b>
<b>6.1.</b>	<b>Architecture Principles .....</b>	<b>52</b>
<b>6.2.</b>	<b>National Command and Control Centre (NCCC) Architecture .....</b>	<b>53</b>
6.2.1.	NCCC Infrastructure Stack.....	53
<b>6.3.</b>	<b>Regional Command and Control Centre (RCCC) Architecture .....</b>	<b>54</b>
<b>6.4.</b>	<b>Local/Edge Command and Control Centre (LCCC) Architecture.....</b>	<b>54</b>
6.4.1.	LCCC Edge Hardware (NOT IN SCOPE OF SDA) .....	55
6.4.2.	Infrastructure .....	55
<b>7.</b>	<b>DETAILED ATMS SOFTWARE STACK.....</b>	<b>57</b>
<b>7.1.</b>	<b>CORE ATMS PROCESSING ENGINE .....</b>	<b>57</b>
7.1.1.	Event Processing Engine (EPE) .....	57
7.1.1.1.	<i>EPE Processing Pipeline .....</i>	<i>58</i>
7.1.1.2.	<i>EPE Performance Requirements.....</i>	<i>59</i>
7.1.2.	Incident Processing Engine .....	59
7.1.2.1.	<i>Incident Lifecycle States .....</i>	<i>59</i>
7.1.3.	Device Communication Engine.....	60
7.1.3.1.	<i>Supported Protocols .....</i>	<i>60</i>
7.1.3.2.	<i>MQTT Topic Structure and Message Standard.....</i>	<i>61</i>
7.1.4.	Command Dispatch Engine .....	62
7.1.5.	Real-Time Stream Processing.....	63
<b>7.2.</b>	<b>UNIFIED NATIONAL GIS PLATFORM.....</b>	<b>63</b>
7.2.1.	GIS Engine.....	63
7.2.2.	Real-Time Traffic Visualization .....	63
7.2.3.	Incident Visualization.....	64

---

7.2.4.	Incident Detection Workflow .....	64
<b>7.3.</b>	<b>NATIONAL API GATEWAY PLATFORM.....</b>	<b>65</b>
7.3.1.	API Gateway Architecture .....	65
7.3.2.	Authentication and Authorization Framework .....	65
7.3.2.1.	<i>Mandatory Government System Integrations (Not only limited to) .....</i>	<i>66</i>
7.3.2.1.1.	VAHAN Integration (Vehicle Registry) .....	67
7.3.2.1.2.	SARATHI Integration (Driver Licence) .....	68
7.3.2.1.3.	FASTag / NETC Integration.....	68
7.3.2.1.4.	Police Enforcement Integration .....	68
7.3.2.1.5.	Court System Integration .....	68
7.3.2.1.6.	State ICCC Integration .....	68
7.3.2.1.7.	Per-Integration Non-Functional Requirements.....	69
<b>7.4.</b>	<b>Vendor Data Interface Layer .....</b>	<b>71</b>
7.4.1.	Vendor Data Interface Layer — Architecture .....	71
7.4.2.	Vendor Interface Catalogue .....	71
7.4.3.	VDIL Technical Standards.....	72
<b>7.5.</b>	<b>NATIONAL DATA LAKE ARCHITECTURE.....</b>	<b>73</b>
7.5.1.	Data Architecture Layers .....	73
7.5.1.1.	<i>Raw Data Zone (Bronze) .....</i>	<i>73</i>
7.5.1.2.	<i>Processed Data Zone (Silver).....</i>	<i>73</i>
7.5.1.3.	<i>Analytics Data Zone (Gold) .....</i>	<i>74</i>
7.5.2.	Data Categories, Volume and Retention.....	74
<b>7.6.</b>	<b>AI and Predictive Analytics Engine.....</b>	<b>75</b>
<b>7.7.</b>	<b>SLA, ASSET, INCIDENT, AND CONTRACT MONITORING ENGINE .....</b>	<b>75</b>
7.7.1.	Asset Registry Data Model.....	76
7.7.2.	SLA Compliance Engine.....	76
<b>7.8.</b>	<b>CYBERSECURITY ARCHITECTURE .....</b>	<b>77</b>
7.8.1.	Zero Trust Architecture .....	78
7.8.1.1.	<i>Zero Trust Principles Applied .....</i>	<i>78</i>
7.8.1.2.	<i>Identity and Access Management (IAM) .....</i>	<i>79</i>
7.8.1.3.	<i>IAM User Roles .....</i>	<i>79</i>
7.8.2.	Encryption Architecture .....	79
7.8.2.1.	<i>Threat Monitoring and SIEM .....</i>	<i>80</i>
<b>7.9.</b>	<b>TESTING AND PERFORMANCE ENGINEERING FRAMEWORK.....</b>	<b>80</b>

---

7.9.1.	Load Testing Architecture .....	80
7.9.2.	Performance Testing Targets .....	80
7.9.3.	Failover and DR Testing .....	81
<b>7.10.</b>	<b>GOVERNANCE AND MONITORING PLATFORM .....</b>	<b>81</b>
7.10.1.	National Dashboard .....	81
7.10.2.	Regional Dashboard.....	81
7.10.3.	Local Dashboard.....	82
7.10.4.	SLA Dashboard .....	82
<b>7.11.</b>	<b>Platform DevOps &amp; CI/CD Environment Architecture.....</b>	<b>82</b>
<b>7.12.</b>	<b>OEM Vendor Sandbox Environment.....</b>	<b>82</b>
<b>7.13.</b>	<b>Integrated Audio Communication Engine .....</b>	<b>83</b>
7.13.1.	Architecture .....	83
7.13.2.	Key Technical Specifications .....	83
<b>7.14.</b>	<b>Report Generation and Analytics Engine .....</b>	<b>84</b>
7.14.1.	Architecture .....	84
7.14.2.	Pre-Built Report Library — Summary.....	84
<b>7.15.</b>	<b>Mobile Application Stack .....</b>	<b>85</b>
7.15.1.	Architecture .....	85
<b>7.16.</b>	<b>Alarm Management Engine .....</b>	<b>85</b>
7.16.1.	Architecture .....	85
<b>7.17.</b>	<b>Road User Information Platform .....</b>	<b>86</b>
7.17.1.	Architecture .....	86
<b>7.18.</b>	<b>Multi-Source Data Fusion Engine.....</b>	<b>86</b>
7.18.1.	Architecture .....	86
<b>7.19.</b>	<b>Weather and Environmental Monitoring Engine.....</b>	<b>87</b>
7.19.1.	Architecture .....	87
<b>7.20.</b>	<b>ATMS Engine Invocation Summary .....</b>	<b>87</b>
<b>8.</b>	<b>WORK PACKAGES AND ITS DELIVERABLES.....</b>	<b>89</b>
<b>8.1.</b>	<b>WORK PACKAGE -1 SCOPE SUMMARY AND KEY DELIVERABLES (YEARS 1 – 5) .....</b>	<b>89</b>
<b>8.2.</b>	<b>WORK PACKAGE 2: SOFTWARE ENHANCEMENTS &amp; PRODUCT EVOLUTION (YEARS 6–10).....</b>	<b>90</b>
8.2.1.	Enhancement Team Composition (Years 6–10) .....	90
8.2.2.	Scope of Software Enhancements .....	90
8.2.3.	WP-2 Key Deliverables .....	91
<b>8.3.</b>	<b>WORK PACKAGE 3: DEPLOYMENT &amp; CORRIDOR INTEGRATIONS (YEARS 1–10).....</b>	<b>91</b>



8.3.1.	Deployment Team Composition (Years 1–10) .....	92
8.3.2.	Phased Rollout Schedule .....	92
8.3.3.	Per-Corridor Onboarding Activities .....	92
<b>8.4.</b>	<b>Work Package 4 — Operations and Maintenance (Years 2–10) .....</b>	<b>93</b>
8.4.1.	WP-4 Bill of Quantities — Operations and Maintenance .....	93
8.4.2.	Staffing Summary — All Periods .....	94
8.4.3.	LCCC Coverage Ratio — Technical Support per Active Corridor .....	94
8.4.4.	Years 2–3 — Technical Support Staffing Detail .....	95
8.4.5.	Years 4–7 — Technical Support Staffing Detail .....	97
8.4.6.	Years 8–10 — Technical Support Staffing Detail .....	99
<b>8.5.</b>	<b>Work Package 5 — Training, Compliance and Specialised Tools .....</b>	<b>100</b>
8.5.1.	WP-5 Bill of Quantities — Training, Compliance and Specialised Tools/Licenses .....	100
<b>9.</b>	<b>FUNCTIONAL REQUIREMENT SPECIFICATION (FRS) .....</b>	<b>102</b>
<b>9.1.</b>	<b>Overview and Purpose .....</b>	<b>102</b>
<b>9.2.</b>	<b>SCOPE BOUNDARY .....</b>	<b>102</b>
<b>9.3.</b>	<b>Three-Tier Deployment Architecture .....</b>	<b>103</b>
9.3.1.	Common GUI Requirements .....	103
9.3.2.	NCCC-Specific GUI .....	106
9.3.3.	RCCC-Specific GUI .....	107
9.3.4.	LCCC-Specific GUI .....	107
<b>9.4.</b>	<b>SECTION A — NINE ATMS POLICY-MANDATED MODULES (NHAI ATMS Policy 2023, Chapter10)</b>	<b>108</b>
9.4.1.	Module 1 — Data Acquisition Module .....	109
9.4.1.1.	<i>Direct Device Data Acquisition</i> .....	110
9.4.1.2.	<i>Vendor Platform Data Ingestion</i> .....	111
9.4.1.3.	<i>Data Pipeline and Storage</i> .....	112
9.4.2.	Module 2 — Highway Traffic Monitoring Module & GIS Dashboard .....	113
9.4.2.1.	<i>Map Platform and Navigation</i> .....	114
9.4.2.2.	<i>Device and Situational Awareness Layers</i> .....	115
9.4.2.3.	<i>Incident and Geofencing Map Tools</i> .....	117
9.4.2.4.	<i>Historical Replay and GIS Data Management</i> .....	118
9.4.3.	Module 3 — Incident / Accident Management Module with Integrated Computer Aided Dispatch (ICAD) .....	119
9.4.3.1.	<i>Incident Detection and Source Integration</i> .....	120
9.4.3.2.	<i>Incident Record and Classification</i> .....	121

9.4.3.3.	<i>Notification and Escalation</i> .....	122
9.4.3.4.	<i>SOP Workflow and Response Orchestration</i> .....	123
9.4.3.5.	<i>Incident Lifecycle, Closure and Analytics</i> .....	124
9.4.4.	Module 4 — Integrated Audio Communication Module .....	126
9.4.4.1.	<i>Unified Communication Interface</i> .....	126
9.4.4.2.	<i>Call Recording and Audit</i> .....	127
9.4.4.3.	<i>In-Platform Messaging and Collaboration</i> .....	128
9.4.5.	Module 5 — Report Generation Module and Dashboard .....	129
9.4.5.1.	<i>Role-Specific Operational Dashboards</i> .....	130
9.4.5.2.	<i>Pre-Built Automated Report Library</i> .....	131
9.4.5.3.	<i>Custom Reporting and Distribution</i> .....	133
9.4.6.	Module 6 — System Administration Module .....	134
9.4.6.1.	<i>User Identity and Authentication</i> .....	134
9.4.6.2.	<i>Role-Based Access Control (RBAC)</i> .....	135
9.4.6.3.	<i>Standard User Role Definitions</i> .....	136
9.4.6.4.	<i>System Configuration Management</i> .....	137
9.4.7.	Module 7 — Communication Module for Authorised Access by External Systems .....	139
9.4.7.1.	<i>Authorised External Access Management</i> .....	139
9.4.8.	Module 8 — API Integrations (VAHAN, CCTNS, NPCI FASTag, NHAI ERP/DataLake, 1033 CAD, Rajmarg, and Existing Field Platform Vendor and other third party DBs as and when required) .....	141
9.4.8.1.	<i>Government &amp; National System Integrations</i> .....	142
9.4.8.2.	<i>Emergency Services and Operational Integrations</i> .....	143
9.4.8.3.	<i>Existing Field Platform Vendor API (Core Integration)</i> .....	145
9.4.9.	Module 9 — Real-Time Equipment Health Monitoring / Network Management System (NMS) ....	146
9.4.9.1.	<i>Asset Registry</i> .....	146
9.4.9.2.	<i>Real-Time Device Health/Status Monitoring</i> .....	147
9.4.9.3.	<i>SLA Monitoring and Penalty calculation</i> .....	148
9.4.9.4.	<i>Fault Management and Maintenance Ticketing</i> .....	149
<b>9.5.</b>	<b>SECTION B — ADDITIONAL SOFTWARE MODULES</b> .....	<b>150</b>
9.5.1.	Module 10 — Open-Source GIS & Mapping Platform (Extended Capabilities) .....	150
9.5.2.	Module 11 — Data Management, Analytics & Intelligence Platform (DMP) .....	151
9.5.2.1.	<i>Data Storage and Lifecycle</i> .....	151
9.5.2.2.	<i>AI and Predictive Analytics</i> .....	152
9.5.3.	Module 12 — Platform Security & Cybersecurity Architecture .....	153

9.5.3.1.	<i>Access Control and Network Security</i> .....	153
9.5.3.2.	<i>Data Encryption and Integrity</i> .....	154
9.5.3.3.	<i>Threat Detection, Monitoring, and Incident Response</i> .....	155
9.5.4.	Module 13 — SLA Monitoring & Asset Lifecycle Management (Extended) .....	156
9.5.5.	Module 14 — Meteorological & Environmental Monitoring Module .....	157
9.5.6.	Module 15 — Mobile Application & Field Operator Interface.....	158
9.5.7.	Module 16 — Alarm Display & Management Module .....	159
9.5.8.	Module 17 — Traffic Data Dissemination to Road Users.....	161
9.5.9.	Module 18 — Multi-Source Data Fusion & Intelligence Summarization .....	162
9.5.10.	Performance and Scale Targets .....	164
<b>10.</b>	<b>PROJECT IMPLEMENTATION TIMELINE – 12 MONTHS</b> .....	<b>165</b>
10.1.	Implementation Timeline Summary .....	165
10.2.	Phase 1 – Project Initiation, Requirement Gathering & SRS approval (T0 to T0+1) .....	165
10.3.	Phase 2 – Development, Integration, and LCCC Rollout (T0+2 to T0+8) .....	165
10.5.	Phase 4 – Full Rollout, Integration Testing, UAT (Wave 1: 150 LCCCs, Wave 2: 250+ LCCCs and Wave 3: 667 LCCs) (T0+12 to T0+120).....	167
10.6.	<b>10-YEARs’ COMPREHENSIVE OPERATIONS &amp; MAINTENANCE FRAMEWORK</b> .....	<b>168</b>
10.6.1.	Cloud Infrastructure Monitoring and Reliability Management.....	168
10.6.2.	O&M Team Composition .....	168
10.6.3.	O&M Service Levels .....	169
10.6.4.	Development-cum-Enhancement Support Team (DEST).....	170
10.6.5.	Annual O&M Activities Calendar.....	171
<b>11.</b>	<b>CYBERSECURITY FRAMEWORK OVERVIEW</b> .....	<b>173</b>
11.1.	Applicable Standards and Directives.....	173
11.2.	<b>SECURE CODE REVIEW &amp; APPLICATION HARDENING</b> .....	<b>173</b>
11.2.1.	Secure Software Development Lifecycle (SSDLC) .....	173
11.2.2.	Secure Code Review (One-Time and Annual) .....	175
11.2.3.	Application Hardening.....	175
11.3.	<b>SIEM DEPLOYMENT AND LOG MANAGEMENT</b> .....	<b>177</b>
11.3.1.	SIEM Platform Requirements.....	177
11.3.2.	Log Management Requirements .....	178
11.4.	<b>ENDPOINT DETECTION AND RESPONSE (EDR)</b> .....	<b>179</b>
11.5.	<b>Identity Access Management (IAM)</b> .....	<b>180</b>
11.6.	<b>Privileged Access Management (PAM)</b> .....	<b>181</b>



11.6.1. Network Segmentation Design .....	182
<b>11.7. CERT-IN / MEITY COMPLIANCE .....</b>	<b>182</b>
11.7.1. One-Time Compliance Activities .....	182
11.7.2. Annual Compliance Obligations .....	183
11.7.3. Cybersecurity License .....	184
<b>12. TRAINING PROGRAMME OVERVIEW .....</b>	<b>186</b>
12.1. Training Target Audience.....	186
12.2. INITIAL TRAINING PROGRAMME (IMPLEMENTATION PHASE)- (Online/Offline) .....	187
12.2.1. Training Modules – Initial Programme .....	187
12.2.2. Training Delivery Methods.....	189
12.2.3. Training Assessment and Certification .....	189
12.3. ANNUAL TRAINING PROGRAMME (O&M PHASE).....	190
12.3.1. Annual Training Calendar .....	190
12.3.2. Annual Training Requirements – By Role .....	191
12.3.3. Training Infrastructure Requirements .....	192
12.4. TRAINING – FUNCTIONAL REQUIREMENTS SUMMARY .....	194
<b>13. BILL OF QUANTITIES (BoQ) FRAMEWORK .....</b>	<b>196</b>
13.1. WP-1 — Core Platform Architecture & Development (Years 1–5) .....	196
13.2. WP-2 — Software Enhancements & Product Evolution (Years 6–10) .....	197
13.3. WP-3 — Deployment & Corridor Integrations (Years 1–10) .....	197
13.4. WP-4 — Operations & Maintenance (Years 1–10) .....	197
13.5. WP-5 — Training, Compliance & Specialized Tools.....	198
<b>SCHEDULE A — SERVICE LEVEL AGREEMENT.....</b>	<b>199</b>
<b>1. Key Terms and Definitions.....</b>	<b>199</b>
1.1. Platform Availability / Uptime .....	199
1.2. National Command & Control Centre (NCCC).....	199
1.3 Regional Command & Control Centre (RCCC) .....	199
1.4 Local Command & Control Centre (LCCC) .....	199
1.5 Incident Response Time .....	199
1.6 Incident Resolution Time .....	200
1.7 Data Processing Latency .....	200
1.8 Disaster Recovery — RTO and RPO.....	200
1.9 SIEM and CSOC .....	200
1.10 CERT-In Reporting Obligation.....	200

<b>1.11 Government Integration Uptime.....</b>	<b>200</b>
<b>1.12 Security Patch Deployment.....</b>	<b>201</b>
<b>1.13 Annual DR Test .....</b>	<b>201</b>
<b>1.14 Annual Operator Training Compliance .....</b>	<b>201</b>
<b>2.1 Measurement Architecture.....</b>	<b>202</b>
<b>2.2 Monthly SLA Report .....</b>	<b>202</b>
<b>2.3 SLA Deduction Mechanics — Monthly to Quarterly.....</b>	<b>202</b>
Table 3.1 — SLA Parameter Quick Reference .....	204
<b>3.1 Category A — Platform Availability.....</b>	<b>205</b>
<b>3.2 Category B — Incident Response &amp; Resolution .....</b>	<b>208</b>
<b>3.3 Category C — Software Performance.....</b>	<b>210</b>
<b>3.4 Category D — Cybersecurity .....</b>	<b>210</b>
<b>3.5 Category E — External Integrations .....</b>	<b>211</b>
<b>3.6 Category F — Disaster Recovery .....</b>	<b>212</b>
<b>3.7 Category G — Compliance &amp; Governance .....</b>	<b>213</b>
<b>4. O&amp;M Fault Categories — Definitions and Financial Penalties.....</b>	<b>215</b>
<b>5. RESOURCE PENALTY FRAMEWORK — RATES AND TRIGGERS.....</b>	<b>228</b>
5.1 Tier 1 — Critical Role Vacancy Penalty.....	228
5.2 Tier 2 — Standard Role Shortfall Penalty.....	229
5.3 Tier 3 — LCCC Field Coverage Ratio Penalty.....	230
<b>6. WP-2 ENHANCEMENT TEAM — MAN-MONTH DELIVERY PENALTY .....</b>	<b>231</b>
6.1 Measurement Method.....	231
6.2 WP-2 Man-Month Shortfall Penalty Rates.....	231
<b>7. WP-3 DEPLOYMENT TEAM — RESOURCE AVAILABILITY PENALTY.....</b>	<b>233</b>
7.1 Measurement Method.....	233
7.2 WP-3 Man-Month Shortfall Penalty Rates.....	233
<b>8. DEPLOYMENT VERIFICATION AND REPORTING .....</b>	<b>235</b>
8.1 Monthly Resource Deployment Report .....	235
8.2 IHMCL Audit Rights .....	235
<b>9. Penalty Calculation — Worked Examples.....</b>	<b>236</b>
9.1 P1 Penalty Calculation .....	236
9.2 Uptime Penalty Calculation.....	236
9.3 Penalty Cap.....	236
<b>10. Measurement, Reporting and Governance.....</b>	<b>237</b>

<b>10.1 Monthly SLA Report .....</b>	<b>237</b>
<b>10.2 Real-Time Monitoring .....</b>	<b>237</b>
<b>10.3 Dispute Resolution .....</b>	<b>237</b>
<b>10.4 Exclusions.....</b>	<b>237</b>
<b>APPENDIX D – ABBREVIATIONS AND GLOSSARY (ADDENDUM) .....</b>	<b>238</b>

## LIST OF FIGURES

Figure 1: Three Tier Architecture Understanding .....	31
Figure 2: Integration Architecture .....	32
Figure 3: Technical Network Architecture.....	33
Figure 4: Three Level Command Hierarchy .....	47
Figure 5: NCCC Functional Use Cases.....	48
Figure 6: RCCC Functional Use Cases.....	49
Figure 7: LCCC Functional Use Cases .....	50
Figure 8: Three Tier Operational Function Overview .....	51
Figure 9: Representation of Enterprise Software Architecture - Layered View .....	53
Figure 10: LCCC Edge Architecture & Autonomous Operation Mode .....	56
Figure 11: ATMS Software Stack with Core Processing Engines .....	57
Figure 12: Event Processing Engine (EPE) — Data Flow Pipeline .....	58
Figure 13: Incident Lifecycle — State Machine Diagram .....	60
Figure 14: ATMS Normal Operations Data Flow .....	62
Figure 15: National API Gateway Integration Architecture .....	66
Figure 16: ATMS Violation Detection and Processing Flow (Step 1 to 4 would happen at Vendor provided VIDES system).....	70
Figure 17: ATMS Incident Response Flow .....	71
Figure 18: Cyber Security Framework.....	78
Figure 19: ATMS Engine Invocation: Which Engine Fires at each Tier .....	88
Figure 20: Nine (9) Policy-Mandated Modules .....	109
Figure 21:Nine (9) Additional Modules.....	150
Figure 22: Governance, Compliance & 10-Year Sustainability .....	173

## 1. KPI Achievement Framework

### 1.1. Preamble

Unified NHAI ATMS Software to be deployed by IHMCL under this RFP is not a passive monitoring system. It is the active enforcement, safety, and governance engine of India's national highway network. The Implementation Agency (IA), which is simultaneously termed as the Software Development Agency (SDA) in this document, is not merely a technology vendor delivering features against a specification. The SDA is the architect of measurable, time-bound highway safety outcomes — outcomes that are legally, operationally, and publicly accountable.

Every module the SDA designs, every API integration the SDA implements at an LCCC, and every AI model the SDA trains must be expressly oriented toward one purpose: enabling the highway system to achieve the KPIs defined in this section. Every KPI has a follow-through process that also needs to be incorporated. This is the design intent of the Unified NHAI ATMS software.

- It is not sufficient for the platform to detect violations — it must ensure challans are issued. Achieving Safe driving is important
- It is not sufficient for the platform to detect incidents — it must ensure response teams reach the scene within the defined Mean Time to Respond. Saving lives is important.
- It is not sufficient for the platform to generate reports — it must surface actionable intelligence that drives measurable compliance improvement across corridors. Leadership action against generated reports will make our roads safe.

This section defines the ten primary KPIs the ATMS Platform must enable, maps each KPI to the specific SDA deliverables and platform modules responsible, and establishes the measurement and accountability framework under which the SDA's performance will be assessed throughout the contract period.

### 1.2. Platform Design Intent

The following matrix articulates the direct correspondence between each strategic objective of the ATMS programme and the specific platform capabilities the IA is mandated to build. This design intent matrix serves as the authoritative reference for evaluating whether the IA's architectural choices, module specifications, and integration decisions are aligned with the programme's outcome expectations. Every design decision made by the IA during development shall be traceable to one or more rows of this matrix.

Strategic Objective	Platform Capability the IA Must Build	Measurable Outcome the Platform Enables	Operational Intelligence Layer in Platform
<b>Safety — Eliminate Fatal Lane Violations</b>	AI video analytics, IDS, ANPR-based wrong-way detection, automated ICAD dispatch	Near-zero wrong-lane incidents; < 3 min incident detection	Local data Real time handling

Strategic Objective	Platform Capability the IA Must Build	Measurable Outcome the Platform Enables	Operational Intelligence Layer in Platform
<b>Enforcement — Automated Penalty Issuance</b>	End-to-end violation pipeline from detection to e-Challan without human intervention	100% automated challan issuance; full evidentiary audit trail	Local data Real time handling
<b>Throughput — Reduced Congestion via Dynamic Management</b>	Real-time traffic monitoring, VMS-driven dynamic lane messaging, incident clearance dispatch	Reduced clearance times; improved corridor throughput	Local, Regional data Real time handling
<b>Compliance — Public Awareness and Behaviour Change</b>	VMS messaging, FASTag SMS alerts, Rajmarg app integration, compliance analytics	85%+ corridor user compliance within 90 days	Local, Regional, National data Real time & planned handling
<b>Deterrence — Repeat Offender Suppression</b>	Cross-corridor offender analytics fusing FASTag + ANPR history	Habitual offenders flagged within 24 hours; graduated enforcement	Local, Regional, National data Periodic & planned handling
<b>Governance — National Visibility and Accountability</b>	Three-tier NCCC/RCCC/LCCC dashboards, SLA engine, analytics reports, IPR-compliant data lake	Live national situational awareness; monthly KPI reporting to MoRTH	Local, Regional, National data Periodic & planned handling
<b>Scalability — Replication Across 1,46,000 km Network</b>	Standardised WP-3 onboarding, VDIL vendor-neutral integration, vendor sandbox	Per-corridor go-live within 45 days of TSP infrastructure readiness	Local, Regional, National data Planned integration

### 1.3. SDA's Scope Boundary in Achieving KPIs

Before mapping KPIs to SDA deliverables, the scope boundary governing the SDA's accountability must be explicitly stated to prevent misattribution of responsibility and to define the precise operational interface between the SDA and other programme stakeholders.

#### 1.3.1. SDA Responsibility

- Designing, developing, testing, deploying, and operating the ATMS Software Platform and all modules specified in this document.
- Ensuring the software platform ingests, processes, and acts on data from field devices supplied and maintained by Technology Service Providers (TSPs) under separate contracts.
- Implementing all government API integrations (VAHAN, SARATHI, FASTag/NETC, e-Challan, 1033, Rajmarg Yatra etc. as per requirements during contract tenure) in accordance with approved interface specifications.
- Configuring AI analytics models, IDS algorithms, and enforcement pipelines to the performance levels defined against each KPI. Every KPI should have a follow-through process module.
- Maintaining platform availability and performance SLAs (99.5% uptime NCCC; 99.0% LCCC) throughout the contract period.
- Providing KPI performance dashboards and KPI Outcome reports, audit logs, and management reports that enable IHMCL and NHAI to exercise oversight.

### 1.3.2. SDA – Out of Scope

- Design, Procurement, installation, or maintenance of physical field hardware (cameras, VMS boards, ANPR gantries, WIM sensors, radar etc.) — these are TSP responsibilities.
- Enforcement authority action on challans — this is the jurisdiction of StateTraffic Police / State Transport Departments / enforcement authorities, acting on evidence generated by the platform.
- Managed MPLS connectivity between LCCC and RCCC — these are IHMCL-provisioned.
- Access credentials for government APIs (VAHAN, SARATHI, NETC etc.) — these are obtained by IHMCL from the respective agencies; the IA implements the integration once credentials are provided.

The KPIs and SDA mandates defined in this Section 1 scoped exclusively within the SDA's software delivery and operations responsibility. Where a KPI outcome depends on TSP hardware uptime, enforcement authority action, or government API availability, the SDA's accountability is limited to its software contribution within that value chain.

### 1.4. Module-to-KPI Responsibility Mapss

The ATMS Platform's 18 modules collectively form the technical substrate through which every KPI in this section is achieved. The following table maps each critical module to its specific role in KPI achievement and the KPI identifiers it directly enables. This table serves as the primary accountability reference during KPI review meetings, system acceptance testing, and any contractual performance dispute resolution.

ATMS Module	Role in KPI Achievement — Design Mandate	KPIs Enabled
<b>Module 1 — Data Acquisition</b>	Ingests all field sensor data (ANPR, WIM, CCTV, radar, MET etc.) via VDIL into the platform in real time. Foundation of every detection KPI.	<b>KPI-01, 04, 08</b>



ATMS Module	Role in KPI Achievement — Design Mandate	KPIs Enabled
<b>Module 2 — Traffic Monitoring &amp; GIS</b>	Provides real-time corridor situational awareness, incident visualisation, and operator map interfaces at LCCC/RCCC/NCCC.	<b>KPI-01, 02, 07</b>
<b>Module 3 — Incident Management / ICAD</b>	Classifies, records, dispatches, and tracks every violation and incident. Core enforcement execution engine. Every incident KPI violation is also managed to closure.	<b>KPI-01, 02, 04, 05, 06, 07, 08</b>
<b>Module 4 — Audio Communication</b>	Enables immediate multi-party voice coordination between TMC, patrol, and emergency services during incidents.	<b>KPI-07</b>
<b>Module 5 — Report Generation &amp; Dashboard</b>	Provides all KPI performance dashboards, daily enforcement reports, MTTD/MTTR tracking, and compliance analytics. All report follow through actions to be managed.	<b>KPI-01 to 10 (all)</b>
<b>Module 7 — External Communication</b>	Exposes ATMS data to authorised external systems: Rajmarg Yatra app, Telecom Companies, State ICCCs, media cells, and future corridor integrators etc.	<b>KPI-09, 10</b>
<b>Module 8 — API Integrations</b>	Connects to VAHAN, SARATHI, FASTag/NETC, e-Challan platforms, 1033 CAD, and Transport Dept systems. Enforcement backbone.	<b>KPI-01, 04, 05, 06, 08, 09</b>
<b>Module 9 — NMS / Equipment Health</b>	Tracks ATMS field device and platform health, SLA compliance, and generates automated maintenance tickets.	<b>KPI-03 (platform readiness)</b>
<b>Module 11 — Data Lake &amp; Analytics / AI</b>	Stores entire national violation, incident, and traffic history. Runs repeat-offender analytics, compliance trends, and predictive models. Repeat offender reports to be shared and actions managed on system.	<b>KPI-02, 05, 06, 09, 10</b>
<b>Module 13 — SLA Monitoring &amp; Asset Lifecycle</b>	Automates SLA measurement against committed service levels and triggers penalty computation for OEM/TSP non-performance.	<b>KPI-03, 07 (response SLAs)</b>
<b>Module 15 — Mobile Application</b>	Equips patrol and RPV teams with geo-fenced incident alerts, status update tools, and navigation — reducing physical MTTR.	<b>KPI-07</b>

ATMS Module	Role in KPI Achievement — Design Mandate	KPIs Enabled
<b>Module 17 — Road User Communication</b>	Manages VMS content authoring and publishing, providing dynamic advisory, diversion, and penalty messaging to corridor users.	<b>KPI-08, 09</b>
<b>Module 18 — Multi-Source Data Fusion</b>	Synthesises ANPR, FASTag, WIM, weather, and violation data into composite intelligence layers for compliance indexing.	<b>KPI-09</b>

### 1.5. KPI / Outcome Expectations — SDA Platform Delivery Obligations

The following table defines the ten primary KPIs the ATMS Platform is designed to achieve. For each KPI, the table specifies: the measurable performance target, the specific SDA software design and configuration obligations that enable that target, and the ATMS modules responsible. These are not aspirational statements — they are contractual platform delivery obligations of the SDA, against which platform acceptance, SLA payments, and performance reviews shall be conducted.

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
<b>KPI-01</b>	<b>Zero Wrong-Lane Cruising Incidents per 100 km</b>	Near Zero incidents per 100 km within 45 days of platform go-live on any corridor	<ul style="list-style-type: none"> <li>SDA shall configure the AI Video Analytics Engine within Module 1 (Data Acquisition) to execute real-time lane-boundary detection at sub-second latency using ANPR and AI-camera feeds ingested over the VDIL.</li> <li>SDA shall build automated geo-tagged violation docket generation within Module 3 (Incident Management / ICAD), triggering immediate classification, evidence attachment, and dispatch.</li> <li>SDA shall ensure the TMC dashboard (Module 2 — Traffic Monitoring &amp; GIS) surfaces live wrong-lane alerts with corridor map overlays to LCC operators within 5 seconds of detection.</li> <li>SDA shall integrate the violation docket pipeline with Module 8 (API Integrations) to push evidence packages to the e-</li> </ul>	<b>M1 – Data Acquisition</b> <b>M2 – Traffic Monitoring &amp; GIS</b> <b>M3 – Incident Management / ICAD</b> <b>M8 – API Integrations</b>

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
			<p>Challan platform without manual intervention.</p> <ul style="list-style-type: none"> <li>SDA shall integrate with telecom operators and other private vehicle platforms on aggregators to ensure messages are delivered to the vehicle.</li> </ul>	
KPI-02	<b>30% Reduction in Lane-Violation-Attributable Accidents within 3 Months</b>	Demonstrated 30% reduction in accidents attributable to lane violations within 90 days of enforcement activation via communication (VMS) and deterrence (challans)	<ul style="list-style-type: none"> <li>SDA shall deploy the Incident Detection System (IDS) algorithms within Module 3 capable of classifying incident types (collision, near-miss, stopped vehicle, wrong-way vehicle) automatically from sensor data streams.</li> <li>SDA shall build crash trend analytics dashboards in Module 5 (Report Generation) enabling Project Directors and NHAI to track accident causation patterns correlated with lane-violation events.</li> <li>SDA shall configure CCTV analytics within Module 2 to feed the IDS with video-based confirmation of detected incidents for evidence-grade logging.</li> <li>SDA shall provide corridor-level accident reduction metrics as a standard pre-built report in Module 5 updated daily for management review.</li> </ul>	<p>M3 – Incident Management / ICAD</p> <p>M2 – Traffic Monitoring &amp; GIS</p> <p>M5 – Report Generation &amp; Dashboard</p> <p>M11 – Analytics &amp; Intelligence</p>
KPI-03	<b>Full-Corridor Regulatory Infrastructure &amp; Platform Operational within 45 Days</b>	ATMS platform operational at all LCCCs on a newly on-boarded corridor within 45 days of physical infrastructure	<ul style="list-style-type: none"> <li>SDA shall complete per-corridor onboarding — MQTT provisioning, VPN setup, certificate issuance, GIS layer update, VDIL pipeline validation, and operator training — within the WP-3 committed per-corridor onboarding timeline.</li> <li>SDA shall configure VMS content management and lane-designation</li> </ul>	<p>M9 – NMS / Equipment Health</p> <p>M17 – Road User Communication</p> <p>M1 – Data Acquisition</p> <p>WP-3 Deployment</p>

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
		readiness certificate from TSP	<p>messaging workflows within Module 17 (Traffic Data Communication to Road Users) to publish regulatory signage instructions to field VMS boards.</p> <ul style="list-style-type: none"> <li>• SDA shall activate Module 9 (Equipment Health Monitoring / NMS) uptime dashboards for the corridor from Day 1, ensuring ATMS health is visible to LCCC, RCCC, and NCCC simultaneously.</li> <li>• SDA shall produce a corridor-readiness certificate upon successful Site Acceptance Test (SAT) validating all 18 modules are operational on the corridor.</li> </ul>	
<b>KPI-04</b>	<b>100% Automated Lane Violation Detection and Documentation from Day 1</b>	Zero manual intervention required for violation detection, evidence capture, and docket generation from commissioning date	<ul style="list-style-type: none"> <li>• SDA shall implement edge-processing capability within the LCCC software stack so that ANPR-based lane-violation detection, AI analytics processing, and initial docket creation execute locally even if WAN connectivity to RCCC is degraded.</li> <li>• SDA shall build the automated violation record schema within Module 3 covering: timestamp, GPS coordinates, vehicle registration, lane ID, violation type, photographic and video evidence, and detection confidence score.</li> <li>• SDA shall ensure the Event Processing Engine (EPE) within the Core ATMS Processing Layer handles violation events at defined throughput without dropping events during peak traffic loads.</li> <li>• SDA shall integrate violation records with Module 8 API pipelines to VAHAN for vehicle owner identification within the defined SLA.</li> </ul>	<p><b>M1 – Data Acquisition</b></p> <p><b>M3 – Incident Management / ICAD</b></p> <p><b>M8 – API Integrations</b></p> <p><b>Core EPE</b></p>

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
KPI-05	<b>100% Automated e-Challan Issuance for All Detected Violations</b>	Every detected and confirmed lane violation results in an automated e-Challan dispatch with zero manual triggering	<ul style="list-style-type: none"> <li>SDA shall design and implement the complete violation-to-challan pipeline: ATMS detection → evidence packaging → VAHAN owner lookup (Module 8) → e-Challan platform API push → acknowledgement logging.</li> <li>SDA shall build a challan issuance reconciliation dashboard in Module 5 showing daily: violations detected, dockets generated, VAHAN lookups completed, challans dispatched, and failure exceptions requiring intervention.</li> <li>SDA shall implement the MParivahan / regional e-Challan platform integration under Module 8 (API Integrations) ensuring compliance with NIC-prescribed API standards and legal evidentiary requirements under IT Act, 2000.</li> <li>SDA shall maintain an end-to-end audit trail from detection event to challan dispatch in the National Data Lake, retained per the data retention schedule.</li> </ul>	<p>M8 – API Integrations (VAHAN, e-Challan)</p> <p>M5 – Report Generation</p> <p>M11 – Data Lake / Analytics</p> <p>M3 – Incident Management</p>
KPI-06	<b>Detection and Escalated Enforcement of Repeat and Habitual Offenders</b>	All repeat offenders (3+ violations within 30 days) automatically flagged with enforcement authority escalation within 24 hours	<ul style="list-style-type: none"> <li>SDA shall build a repeat-offender analytics engine within Module 11 (Data Management, Analytics &amp; Intelligence Platform) correlating FASTag transaction records (via Module 8 NETC integration) with ANPR violation history to identify habitual offenders across corridors and sessions.</li> <li>SDA shall design the offender profile data model in the National Data Lake to persist violation history per vehicle registration number across the entire national highway network.</li> </ul>	<p>M11 – Analytics &amp; Intelligence</p> <p>M8 – FASTag / NETC Integration</p> <p>M3 – Incident Management / ICAD</p> <p>M5 – Reporting</p>

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
			<ul style="list-style-type: none"> <li>• SDA shall build automated escalation workflows within Module 3 (ICAD) that generate enforcement authority notifications when a vehicle registration crosses defined repeat-violation thresholds.</li> <li>• SDA shall provide fleet-level analytics in Module 11 for commercial vehicle operators through information received from ANPR Camera fetching through NIC / Vahaan Database, enabling transport departments to identify high-risk fleets.</li> </ul>	
KPI-07	<b>MTTD &lt; 3 Min / MTTR &lt; 10 Min for All Corridor Incidents</b>	Mean Time to Detect (MTTD) under 3 minutes; Mean Time to Respond (MTTR) under 10 minutes for all P1 incidents	<ul style="list-style-type: none"> <li>• SDA shall configure the Incident Detection System within Module 3 with AI-driven automatic incident classification covering: accidents, stopped vehicles, wrong-way drivers, debris, and congestion events — reducing detection to automated threshold triggers, eliminating human polling delays.</li> <li>• SDA shall implement Computer-Aided Dispatch (ICAD) workflows in Module 3 that automatically generate response task assignments to the nearest available patrol/RPV team within 30 seconds of confirmed incident detection.</li> <li>• SDA shall configure the Mobile Application (Module 15) for field operators to receive geo-fenced incident alerts with real-time navigation and update incident status from the field, feeding live MTTR tracking back into the TMC.</li> <li>• SDA shall build MTTD and MTTR performance dashboards in Module 5 as</li> </ul>	<p>M3 – Incident Management / ICAD</p> <p>M4 – Audio Communication</p> <p>M15 – Mobile Application</p> <p>M5 – Reporting</p> <p>M2 – GIS Dashboard</p>



KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
			<p>mandatory daily KPI metrics reviewed at LCC, RCC, and NCC levels.</p> <ul style="list-style-type: none"> <li>SDA shall ensure the Integrated Audio Communication Engine (Module 4) enables single-click conference bridging between TMC operator, patrol team, and emergency services at incident trigger.</li> </ul>	
KPI-08	<b>100% Detection of Overloaded HCVs and Mandatory Weighbridge Diversion</b>	All overloaded HCVs detected at WIM sensors automatically diverted to weighbridge; zero overloaded vehicles cleared without weighbridge check	<ul style="list-style-type: none"> <li>SDA shall integrate Weigh-in-Motion (WIM) sensor data streams into Module 1 (Data Acquisition) via the VDIL, ensuring axle-load and gross-weight data are ingested in real time alongside ANPR captures.</li> <li>SDA shall build the overload detection logic within the Core ATMS Processing Engine so that threshold breaches automatically trigger: ANPR evidence capture, violation docket creation in Module 3, and VMS diversion instruction via Module 17.</li> <li>SDA shall integrate overload violation records with Module 8 pipelines to the Transport Department enforcement system for prosecutorial follow-through.</li> <li>SDA shall provide overload detection analytics fleet wise weight violation — vehicle-wise, axle-configuration-wise, and corridor-wise — within Module 11 to support enforcement planning.</li> <li>Connect vehicle weight violation data at fleet operator level to showcase trends or repeat behaviours</li> </ul>	<p>M1 – Data Acquisition (WIM)</p> <p>M3 – Incident / Violation Management</p> <p>M17 – Road User Communication (VMS)</p> <p>M8 – Transport Dept Integration</p>
KPI-09	<b>85%+ Corridor User Awareness and</b>	Measured 85%+ awareness and	<ul style="list-style-type: none"> <li>SDA shall implement the Road User Information Platform (Module 17) enabling authorised TMC operators to</li> </ul>	M17 – Road User Communication

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
	<b>Compliance within 90 Days</b>	lane compliance among corridor users within 90 days of platform go-live	<p>publish lane advisory, violation penalty, and safety messages to corridor VMS boards in real time from a single authoring interface.</p> <ul style="list-style-type: none"> <li>• SDA shall build the FASTag-linked notification integration within Module 8 (NETC/FASTag API) to trigger automatic SMS/push alerts to vehicle owners upon violation detection and for general safety advisories.</li> <li>• SDA shall configure the Multi-Source Data Fusion Engine (Module 18) to synthesise compliance trend data from violation rates, WIM readings, and IDS events into a composite compliance index reported in Module 5.</li> <li>• SDA shall provide the Media Cell with API access (Module 7 — External Communication Module) to feed real-time highway status data to public information systems including FM radio integration and Rajmarg Yatra app.</li> </ul>	<p>M8 – FASTag / NETC Integration</p> <p>M7 – External Communication</p> <p>M18 – Data Fusion</p> <p>M5 – Reporting</p>
<b>KPI-10</b>	<b>Documented Benchmark SOP and Replication Readiness for New Corridors</b>	Fully replicable, documented SOP package ready for deployment on any new corridor within 6 months of first corridor go-live	<ul style="list-style-type: none"> <li>• SDA shall consolidate ATMS operational logs, enforcement statistics, detection accuracy metrics, and SLA performance records from the National Data Lake (Module 11) into a structured Corridor Performance Report within Module 5.</li> <li>• SDA shall maintain a versioned WP-3 onboarding playbook covering MQTT provisioning, VDIL pipeline configuration, GIS layer setup, government API activation, and operator certification — updated after each corridor go-live.</li> <li>• SDA shall maintain the OEM Vendor Sandbox Environment to enable rapid</li> </ul>	<p>M5 – Reporting &amp; Dashboard</p> <p>M11 – Data Lake &amp; Analytics</p> <p>M7 – External API</p> <p>WP-3 Onboarding</p> <p>IPR / Documentation</p>

KPI Ref.	KPI / Outcome Expectation	Measurable Target	IA Platform Delivery Obligation — Module-Level Mandates	ATMS Modules Responsible
			<p>validation of new field device types prior to corridor onboarding, reducing onboarding cycle time for future corridors.</p> <ul style="list-style-type: none"> <li>• SDA shall publish API specifications and integration interface documents (via Module 7 / API Gateway) enabling future system integrators and TSPs to self-onboard to the ATMS platform with minimal IA intervention.</li> <li>• SDA shall ensure all source code, architectural documentation, configuration artefacts, and deployment scripts are maintained in version-controlled repositories accessible to IHMCL/NHAI at all times as part of IPR compliance.</li> </ul>	

### 1.6. KPI Measurement, Reporting, and Review — SDA's Platform Obligations

Measurement of KPI achievement is not a separate activity from platform operation — it is a built-in function of the ATMS Platform that the SDA is mandated to design and deliver. The following sub-sections define the SDA's obligations at each reporting cadence. The measurement of these KPIs shall form the basis for the Service Level Agreement (SLA) of the SDA.

#### 1.6.1. Real-Time KPI Visibility (Continuous — Platform Uptime)

- The SDA shall configure the NCCC National Dashboard, RCCC Regional Dashboard, and LCCC Operational Dashboard (Module 5) to surface live KPI metrics including: current violation counts, active incident counts, MTTD/MTTR rolling averages, equipment health scores, and challan issuance rates.
- All dashboard data shall be refreshed within the display latency SLA (< 5 seconds for critical metrics, < 30 seconds for aggregate metrics).
- The SDA shall configure automated alert thresholds in Module 16 (Alarm Management) so that KPI degradation events trigger supervisor notifications without operator intervention.

#### 1.6.2. Daily Automated Reports (Module 5 — Pre-Built Report Library)

- The SDA shall implement the following as mandatory pre-built reports in Module 5, generated automatically at 0600 hrs daily for each corridor and at national level: Lane Violation Summary (by type, corridor, time-of-

day); Incident Register with MTTD/MTTR per event; e-Challan Issuance Reconciliation; Equipment Uptime and NMS Fault Log; WIM Overload Detection Summary.

- Reports shall be distributed automatically to designated recipients (LCCC Supervisor, RCCC Manager, NHAI Project Director, IHMCL NCCC) via email integration without manual trigger.

#### **1.6.3. Monthly KPI Review Package**

- The IA shall produce a Monthly Corridor Performance Report in Module 5 providing trend analysis against each of the 10 KPIs, with variance flagging for any KPI below target.
- The report shall include: month-on-month comparison, corridor-level breakdown, top-10 violation locations (heatmap), top-20 repeat offenders (anonymised for public reporting), and enforcement conversion rate (violations detected versus challans successfully issued and acknowledged).

#### **1.6.4. Quarterly Audit Data Package**

- The SDA shall maintain a queryable audit log in the National Data Lake covering the complete event-to-enforcement trail for every violation record, with data retained per the retention schedule defined in Module 11.
- The SDA shall provide IHMCL with direct read-only query access to the analytics layer of the National Data Lake for independent KPI verification, without requiring IA intermediation.

### **1.7. Platform Replication and SOP for New Corridors**

The Unified NHAI ATMS software's design must be inherently replicable across any new corridor added to the national highway network. The SDA's obligations under Work Package 3 (WP-3) are directly linked to the platform achieving KPI-10 (Benchmark Corridor SOP). The following commitments are binding on the SDA:

- The SDA shall standardise the per-corridor onboarding sequence such that every new LCCC can be brought to operational go-live within 45 days of TSP infrastructure readiness certification, without requiring bespoke software development.
- The SDA shall maintain a live WP-3 Onboarding Playbook, version-controlled and accessible to IHMCL, covering all technical steps from MQTT provisioning through SAT completion.
- The SDA shall operate the OEM Vendor Sandbox environment to validate new field device types from TSPs within 10 business days of submission, reducing integration friction for new corridor deployments.
- The SDA shall ensure all 18 platform modules are pre-configured as templates that can be instantiated for a new corridor with corridor-specific parameters (corridor ID, GIS layers, device inventory, LCCC credentials) without code changes.
- The SDA shall provide IHMCL with full access to source code repositories, build scripts, configuration artefacts, and deployment documentation at all times, ensuring programme continuity and full replication capability independent of any single vendor.

### **1.8. Summary: The Commitment to Outcome-Oriented Platform Design**

The Agency awarded this contract accepts, as a core contractual obligation, that the ATMS Platform being designed and built is not a technology deliverable measured by feature completeness — it is a safety and enforcement infrastructure measured by the real-world outcomes it enables on India's national highways.

The ten KPIs defined, the module-to-KPI accountability matrix, and the measurement obligations collectively constitute the SDA's outcome delivery framework. Every architectural decision — from the choice of stream processing infrastructure in the Core EPE, to the data model of the National Data Lake, to the escalation workflows in the ICAD engine, to the API integration standards for the e-Challan platform — must be made with the singular objective of ensuring these KPIs are achievable, measurable, and sustained across the lifecycle of the contract.

IHMCL and NHAI shall use this section as the primary reference for platform acceptance testing, KPI-linked payment milestones, and performance reviews throughout the ten-year contract period. The IA is expected to proactively surface KPI performance data, propose corrective measures for any underperforming KPI, and treat every detected deficiency as a design or configuration obligation rather than an operational exception.

---

## 2. Broad Scope of Work of Software Development Agency (SDA)

---

The Software Development Agency (SDA) shall design, develop, deploy, operate and maintain the unified, scalable and vendor-agnostics Advanced Traffic Management System (ATMS) Software Stack under the **“One Nation, One ITS”** framework, in alignment with NHAI ATMS Policy 2023 (as amended from time to time), for pan-India deployment across National Highways.

The broad Scope of Work for the SDA shall include, but not be limited to, the following:

**a) Design of System Architecture**

- i. Prepare System Requirement Specifications (SRS), High-Level Design (HLD) and Low-Level Design (LLD) documents in consultation with IHMCL/NHAI.
- ii. Design a modular, plug-and-play, microservices-based, open-sourced, API-first architecture.
- iii. Define integration standards, interface control documents and deployment architecture
- iv. Establish version-controlled interface catalogue for interoperability with multi-vendor field devices and external systems.
- v. Design and provide cloud DR requirements for NCCC software deployment. However, provision of cloud shall not be in scope of SDA.

**b) Software Application Development** - The Software Development Agency (SDA) shall undertake the design, development, configuration, customisation, testing, deployment and commissioning of a comprehensive, modular and multi-tier Advanced Traffic Management System (ATMS) Software Platform, strictly in accordance with the Functional Requirements, Technical Specifications, Standards and Service Level Requirements stipulated in the RFP and any subsequent clarifications issued by IHMCL/NHAI. All developments shall comply with open standards and ensure vendor neutrality.

**c) Pilot Deployment** - The SDA shall deploy the ATMS Software on identified pilot corridors/projects and ensure its configuration, commissioning and stabilisation in coordination with the concerned stakeholders. The SDA shall also support onboarding, interoperability validation and certification of multi-vendor field devices and subsystems in accordance with the prescribed interface standards and testing protocols.

**d) Roll-out of ATMS software and Integration** – The SDA shall facilitate, coordinate and provide comprehensive technical support for phased roll-out and deployment of the ATMS Software Platform across Local Command and Control Centres (LCCCs), Regional ATMS Command and Control Centres (RCCCs) and the National Command and control Centre (NCCC) across various zones and projects. The SDA shall extend necessary software-level integration support, configuration assistance and validation support to respective ATMS System Integrators (SIs) to enable timely stabilisation and successful Go-Live of ATMS projects in different zones/regions.

**e) Integration with external applications** - The SDA shall be responsible for the design, development, implementation and maintenance of integrations between the ATMS Software Platform and external systems as specified in this RFP, including but not limited to Regional e-Challan systems, Rajmarg Yatra



Mobile App, NH Helpline (1033), India's Emergency Response Support System (ERSS), Toll Monitoring and Control Centre (TMCC), etc. and any other applications or platforms as prescribed under the NHAI ATMS Guidelines 2023 (as amended from time to time) during the Contract period. Such integrations shall be undertaken in a secure, standardised and interoperable manner in accordance with the approved interface specifications and technical standards.

- f) **Application Hosting & Management** - The SDA shall design a cloud ready ATMS Software Platform in a hybrid architecture comprising on-premises infrastructure at respective Command and Control Centres (LCCCs and RCCCs) and a centralized (NCCC) cloud environment for DR Site, as approved by IHMCL/NHAI. The application instances at CCCs shall be deployed on designated local servers for operational continuity, while centralised cloud infrastructure shall be utilised for coordinated updates, remote configuration management, central monitoring and over-the-air (OTA) software upgrades.
- g) **Real-Time Equipment Health Monitoring and Incident Management** - The SDA shall design, develop and operationalise a centralized real-time monitoring module within the ATMS Software Platform for continuous tracking of field equipment health status (including uptime/downtime, connectivity, performance and fault alerts) and unified incident reporting, monitoring and lifecycle management across Local CCC, Regional CCC. The system shall provide automated alerts, SLA monitoring, geo-tagged dashboards, audit trails and analytics to enable proactive maintenance, timely incident response and performance oversight across all ATMS projects.
- h) **Cybersecurity and Compliance** - The SDA shall design, implement and maintain the ATMS Software Platform in accordance with a security-by-design framework ensuring compliance with applicable Government of India cybersecurity guidelines and standards, including MeitY/CERT-In advisories, ISO/IEC 27001 (or equivalent information security standards), and any cybersecurity requirements notified by Government of India from time to time during contract tenure. The SDA shall conduct periodic Vulnerability Assessment and Penetration Testing (VAPT), security/forensic audits and compliance reviews.
- i) **Operations & Maintenance** - The SDA shall provide comprehensive O&M services throughout the Contract Period including for the developed and deployed software-
- 24x7 application support and monitoring
  - Preventive and corrective maintenance
  - Periodic upgrades and patches
  - Real time equipment health status, SLA monitoring and reporting
  - Database management and archival strategy
  - Continuous enhancement based on policy and regulatory changes
- j) **Capacity Building & Knowledge Transfer** – The SDA shall undertake comprehensive capacity building and structured knowledge transfer to ensure effective adoption, smooth operation and long-term sustainability of the ATMS Software Platform. This shall include conducting structured training program

for Command & Control Centre (CCC) operators, IHMCL/NHAI officials, O&M contractors and other designated stakeholders, as required under the Contract. The SDA shall prepare and disseminate detailed training manuals, Standard Operating Procedures (SOPs), user guides and e-learning modules, and shall provide complete technical documentation including, but not limited to, source code, system architecture documents, configuration details, interface specifications and deployment manuals. The SDA shall ensure systematic, phased and properly documented knowledge transfer to designated agencies/teams of IHMCL/NHAI to enable independent oversight, administration, future enhancements and continuity of operations during and beyond the Contract period.

- k) **Intellectual Property Rights (IPR)** - All intellectual property rights in respect of the ATMS Software Platform, including but not limited to source code, object code, configurations, custom developments, enhancements, documentation and related artefacts developed under the Contract, shall exclusively vest with NHAI/IHMCL. The SDA shall provide full and unrestricted access to the complete source code repositories, build scripts, technical documentation and related materials to NHAI/IHMCL throughout the Contract period and upon its completion. The core modules of the ATMS Software Platform shall not be subject to proprietary lock-in, and the solution shall be designed in a manner that enables NHAI/IHMCL to independently operate, maintain, enhance or transition the system to another agency without technical or contractual restrictions, subject to applicable third-party licensed components explicitly disclosed in the bid. SDA shall ensure that all components delivered are free from third-party claims and shall provide necessary licenses for any third-party software used. NHAI/IHMCL shall have perpetual, unrestricted rights to use, modify, enhance, replicate, and deploy the solution without any additional cost or dependency on the SDA.
- l) **Exit Management and Transition Support** - Upon expiry or termination of the Contract, the SDA shall ensure an orderly and seamless transition of the ATMS Software Platform and associated services. The SDA shall provide complete and updated documentation, source code repositories, configurations, system artefacts, deployment scripts, credentials (as per approved handover protocol), and all relevant technical and operational materials necessary for continued operation of the system. The SDA shall extend full cooperation and transition support to IHMCL/NHAI or any agency designated by them, including technical handholding, knowledge transfer sessions and migration assistance, to ensure continuity of services without disruption during the transition period.

---

### 3. Programme Overview and Strategic Context

---

The Indian Highway Management Company Limited (IHMCL), operating under the National Highways Authority of India (NHAI) and the Ministry of Road Transport and Highways (MoRTH), is procuring a unified, enterprise-grade National Advanced Traffic Management System (ATMS) Software Platform. The platform will serve as the exclusive digital command and intelligence layer across India's entire National Highway network, presently spanning over 1,46,000 km and projected to expand to 2,00,000 km by 2030.

This procurement is structured as a long-term managed service contract of up to 10 years and is among the largest government technology service engagements in the Indian transportation sector. The Implementation Agency (IA) or Software Development Agency (SDA) awarded this contract will be the single authoritative software partner for NHAI's highway operations for the duration of the agreement for designing, building, deploying, operating, and continuously evolving the platform that manages the safety and efficiency of one of the world's largest highway networks.

This Enterprise National ATMS Software Specification defines the complete software blueprint for the national ATMS programme. It aligns with NHAI's ATMS Policy 2023 (Chapter 7), and global best practices from FHWA (USA), Highways England (UK), Transport for NSW (Australia), and the EU DATEX II framework.

The system is designed to scale beyond 1000,000 field devices, process data from more than 10 million vehicles per day and provide seamless interoperability with national databases including VAHAN (vehicle registry), SARATHI (driver licence), FASTag (electronic toll collection), NIC systems, Rajmargyatra, police enforcement platforms, court management systems, and State Integrated Command and Control Centres (ICCCs).

#### 3.1. Programme Objectives

The National ATMS Programme has been established to achieve the following strategic objectives:

- To develop and deploy a unified, NHAI-owned ATMS software platform across all NHAI stretches and control rooms with monitoring capability from Ros and central level.
- Common features and seamless integration with various government and third-party applications, serving as a common interface for interconnection of multiple government platforms to enable prompt response and effective mitigation during emergencies.
- Enhance road safety by providing real-time incident detection, traffic monitoring, and automated enforcement across the national highway network.
- Reduce traffic congestion through dynamic traffic management, variable message dissemination, and integrated corridor management.
- Improve road user experience through real-time information provision, faster emergency response, and reduced enforcement friction.
- Enable revenue assurance through integration with FASTag and enforcement of traffic violations linked to court and penalty systems if required.
- Establish a unified National Command and Control architecture enabling NHAI, Ministry of Road Transport and Highways (MoRTH), and State governments to exercise joint oversight.

- 
- Achieve compliance with all applicable Indian standards, cybersecurity directives (CERT-In, NCIIPC), and internationally recognised ITS standards.

### 3.2. Scope of This Document

This specification covers primarily:

- **Policy Compliance and System Overview:** Executive summary, national operational concept, and command hierarchy.
- **Enterprise Software Architecture:** Detailed technical architecture covering AI, GIS, API gateway, data lake, cybersecurity, and governance platforms.
- **Functional Requirement Specification (FRS):** Over 500 numbered functional requirements covering all ATMS subsystems and integrations.

### 3.3. Architectural Mandate — Three-Tier Command Structure

The platform is architecturally mandated to operate concurrently across three distinct tiers of command authority:

- **National Command & Control Centre (NCCC)** — a single, pan-India operations hub providing real-time national situational awareness, strategic incident management, cross-regional escalation authority, and consolidated analytics reporting to MoRTH and Parliament.
- **Regional Command & Control Centres (RCCCs)** — approximately, about 20 RCCCs, each managing a defined geographic zone of the national network, responsible for regional incident escalation, cross-LCCC corridor event coordination, and zone-level operational oversight.
- **Local Command & Control Centres (LCCCs)** — over 667 LCCCs distributed at approximately every 75–100 km along the national highway network, each directly interfacing with the field infrastructure and serving as the primary point of operational response.

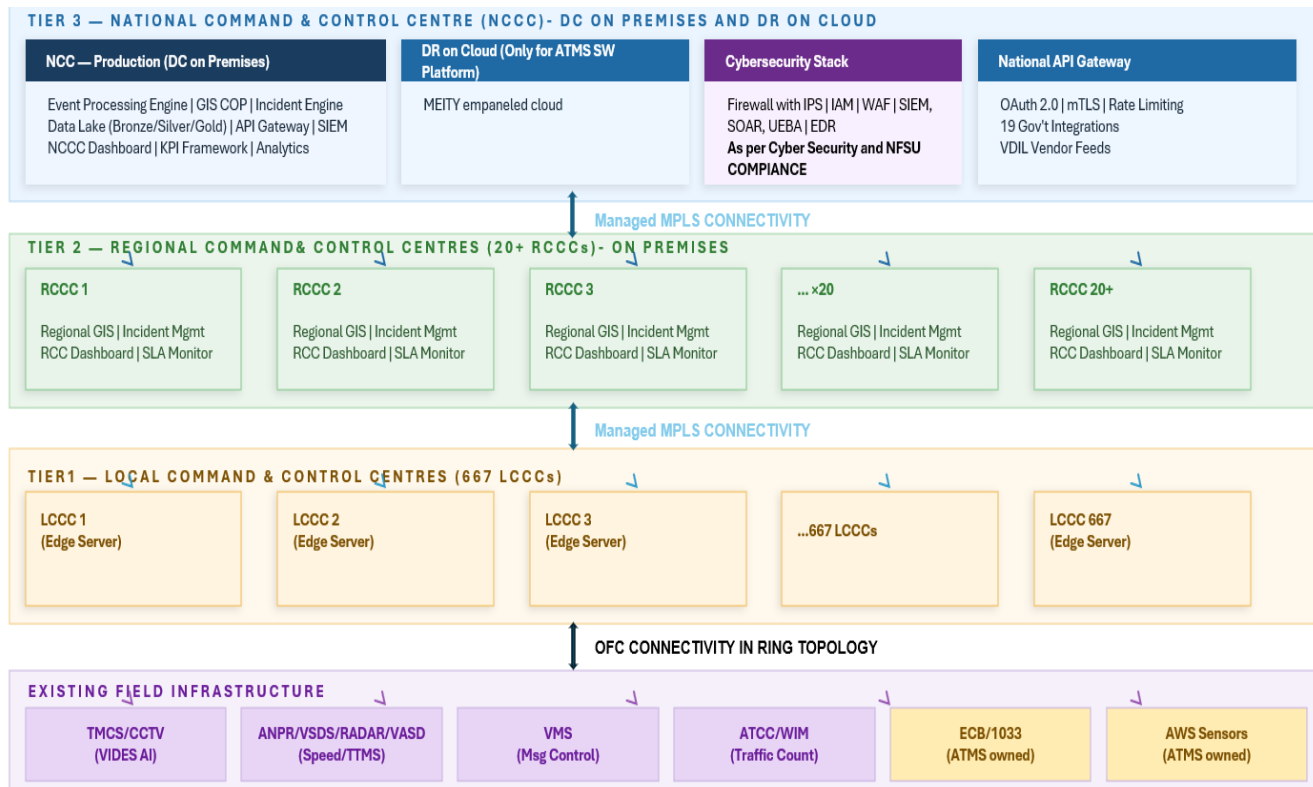


Figure 1: Three Tier Architecture Understanding

All three tiers must operate under similar GUI guidelines catering to each user-role, sharing a common data lake, and maintain seamless, real-time escalation of incidents and commands across all levels. The platform must be cloud-native, built and hosted exclusively on-premise with Disaster Recovery on a MEITY-empaneled Indian Cloud infrastructure as per the latest MEITY guidelines for cloud, and must integrate in real time with national government databases including VAHAN, SARATHI, FASTag/NETC, Rajmargyatra, police systems, e-Courts, and State ICCCs as well as any other third-party databases as mandated from time to time NHAI/IHMCL shall provide the necessary support and facilitation for enabling such integrations.

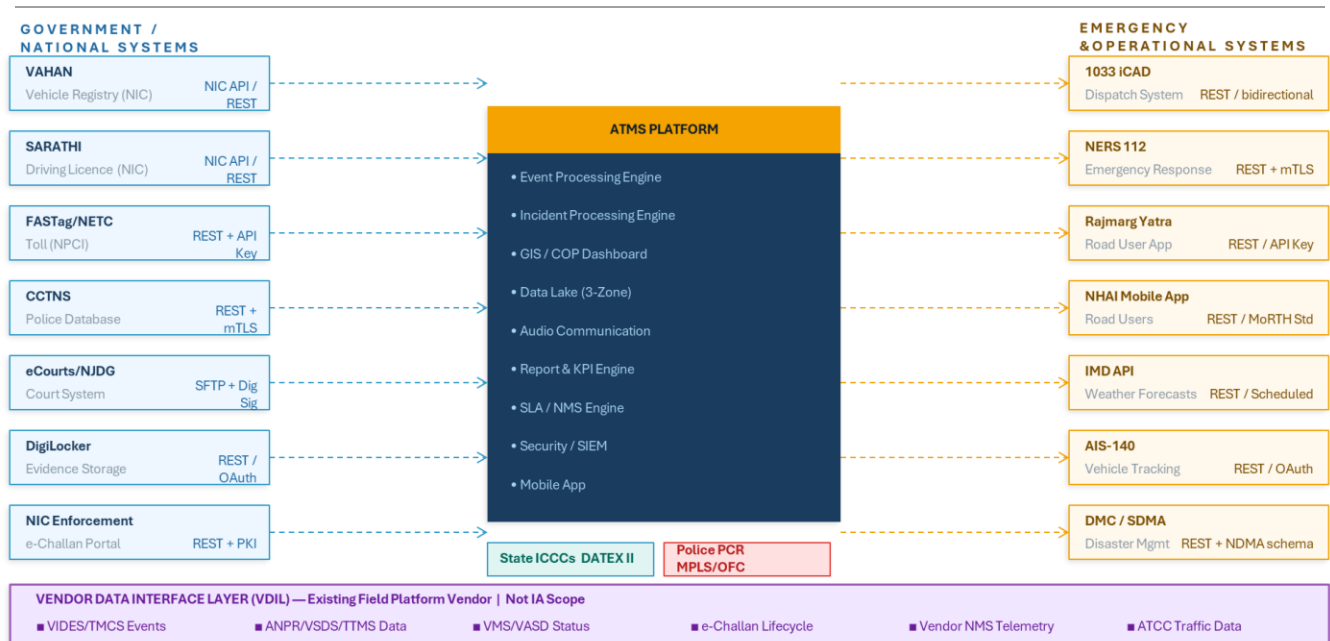


Figure 2: Integration Architecture

### 3.4. Technical Network Architecture

At the highest level is the National Command and Control Centre (NCCC), acting as the central hub hosted both in the cloud (DR) and on-premises (DC). This tier connects via a Managed MPLS network to 20 Regional Command and Control Centres (RCCCs), which serve as intermediate distribution hubs. Each regional center manages a specific group of the 667+ Local Command and Control Centres (LCCCs)—for example, RCCC 1 oversees LCCCs 1 through 25. Finally, at the ground level, these local centers use optical fiber cables (OFC) to connect directly to Field Infrastructure, which includes surveillance cameras, radar units, and Variable Message Display (VMD) boards used for real-time traffic monitoring and data collection.



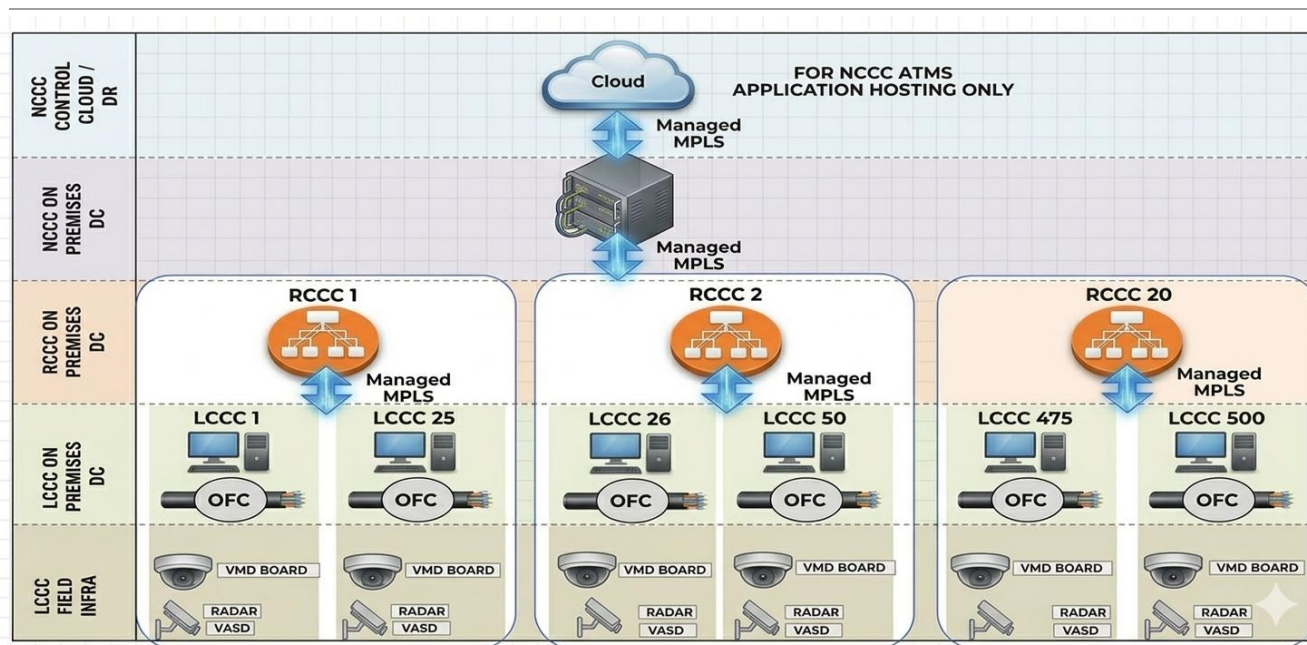


Figure 3: Technical Network Architecture

### 3.5. Work Package Structure

The National ATMS Platform contract is structured across five Work Packages:

WP	Work Package	Duration	Pricing Basis	IA Accountability
WP-1	Core Platform Architecture & Development	Years 1–5	Lump Sum + Man-Month	Full software platform — all modules — designed, built, tested, and stabilised. Year 1- delivery of production-grade platform; Years 2–5 stabilisation, defect remediation, and minor enhancements.
WP-2	Software Enhancements & Product Evolution	Years 6–10	Retainer	Annual major releases and quarterly minor releases. AI model retraining bi-annually. Absorption of regulatory and API changes.
WP-3	Deployment & Corridor Integrations	Years 1–10 (ongoing)	Man-Month + Per-Corridor Unit Rate	Onboarding of new LCCs as NHAI expands the highway network. Per-corridor unit rate covers VPN setup, MQTT configuration, certificate provisioning, GIS update, pipeline validation, operator training, and SAT.
WP-4	Operations & Maintenance — Managed Service	Years 1–10 (ongoing)	Monthly Managed Service Fee	NOC operations. P1 fault response within 15 minutes; resolution within 4 hours. Bug Fixes, Application Support, LCCC/RCCC/NCCC

WP	Work Package	Duration	Pricing Basis	IA Accountability
				Support, Ongoing Integrations, DR testing, patch management, and capacity planning.
<b>WP-5</b>	Training, Compliance & Specialised Tools	Throughout contract	Per Programme / Per Assessment	Annual CERT-In VAPT. ISO 27001:2022 certification and maintenance. 20 training programmes over 10 years across all tiers. Security tool licence management.

### 3.6. 1,200 KM CORRIDOR DEPLOYMENT — RESPONSIBILITIES & WORKFLOW

*e.g.. Delhi–Mumbai Expressway Illustrative Example · IHMCL / IA / Field TSP*

It provides a structured, step-by-step walkthrough of how the National ATMS Platform is deployed on a representative 1,200 km national highway corridor — from Day Zero through to full operational go-live — with explicit definition of what each of the three principal stakeholders is responsible for at every stage. This section is provided to enable prospective bidders to accurately scope their WP-3 unit rate, understand the dependencies that govern their deployment timeline, and avoid the most common causes of dispute and overrun in ATMS corridor deployment programmes.

The example corridor used throughout this section is the Delhi–Mumbai Expressway (1,200 km, illustrative). All quantities and timelines are indicative and are provided solely for planning and understanding purposes.

#### 3.6.1. Infrastructure Already In Place — What the SDA Inherits

For any corridor being on-boarded to the National ATMS Platform, it can be assumed that the physical field infrastructure shall already have been installed and commissioned under a separate NHAI/IHMCL field contract prior to the SDA commencing onboarding activities. The typical infrastructure profile for a 1,200 km corridor is as follows:

Parameter	Basis of Calculation	Estimated Value
<b>VIDES/ANPR Gantries</b>	1 gantry every 5–10 km along 1,200 km corridor. 2/3 cameras shall be installed per gantry.	~120–240 gantries
<b>TMCS/CCTV Cameras</b>	~1 PTZ camera at every KM	~1200 PTZ cameras
<b>VMS Boards</b>	~1 EN 12966-compliant VMS unit per gantry	~120 VMS units
<b>VASD</b>	~1 per gantry	~120-240 VASD units
<b>Radar</b>	~1 per gantry	~120-240 radar sensors

Parameter	Basis of Calculation	Estimated Value
<b>Meteorological System</b>	1 per 100 KM Stretch/LCCC	~12 weather stations if available
<b>Emergency Call Boxes (ECB) if available</b>	1 per 2 km	~600 ECB Pair if available
<b>Local Control Centres (LCCC)</b>	1 per 100 km with necessary infra (IT, Non-IT, Cooling, Fire, Access, etc.), civil and electrical works and Furniture, fully fitted with rack, power, A/C	12 LCCCs
<b>Network Connectivity (per LCCC)</b>	Field to LCCC: Dark Fibre LCCC to RCCC: Managed MPLS with dual redundant connectivity links (100 Mbps) as a primary network connectivity medium and OFC connectivity shall be connected as a secondary network medium, wherever feasible, to ensure redundancy and reliability.	IHMCL-provisioned

### 3.6.2. The Three Principal Stakeholders — Roles and Authorities

#### STAKEHOLDER 1: IHMCL / NHAI — The Employer and Project Authority

Indian Highway Management Company Limited and NHAI. The project authority, contract owner, and entity ultimately accountable to MoRTH and Parliament for the ATMS programme. IHMCL is the client for both the SDA, software contract and all field hardware TSP contracts.

- Owns all hardware assets — cameras, drones (if available), gantries, VMS, sensors, ECBs — procured and maintained under separate TSP contracts.
- Owns and provides the LCCC buildings, stable power supply infrastructure, and rack space at each LCCC.
- Owns and provisions the WAN connectivity (Managed MPLS circuits) between LCCCs and RCCCs through reputed ISP.
- Holds and provisions all government API access credentials — VAHAN, FASTag, police systems — obtained through inter-ministerial MoUs.
- Governs the SLA performance of both the IA and all field TSPs through the ATMS platform dashboards.
- Approves all major software releases, configuration changes, and corridor onboarding milestones.

- 
- Staffs and operates the NCCC and all RCCCs with IHMCL-employed or IHMCL-contracted operations personnel.

**STAKEHOLDER 2: THE SOFTWARE DEVELOPMENT AGENCY (SDA) — The Software Vendor**

The company or consortium awarded this tender. Solely and exclusively responsible for designing, building, deploying, operating, and continuously improving the National ATMS Software Platform for the full 10-year contract duration.

- Designs, builds, unit-tests, integrates, and acceptance-tests the complete ATMS software platform across all 18 functional modules (WP-1).
- Provisions, configures, and install on the MEITY-empanelled cloud (Provided by NHAI/IHMCL) infrastructure hosting the NCCC platform and related components for Disaster Recovery (DR).
- Develops and sustains all mandatory government API integrations across the full contract term.
- Deploys the ATMS LCCC Agent software on the edge servers provided by IHMCL at each LCCC via automated CI/CD pipeline or any other way as per project timelines and SLA.
- Configures and maintains the MQTT broker architecture, device certificate infrastructure (PKI/CA), and data ingestion pipeline for every corridor.
- Operates the 24×7 NOC for the software platform — cloud health, API integration availability, AI inference latency, and LCCC agent connectivity. Does NOT perform field hardware maintenance.
- Provides the SLA monitoring dashboard and calculation of Monthly/Quarterly penalties used by IHMCL to govern the performance of all field TSPs against their contractual obligations including LCCC, RCCC and NCCC.
- Designs and delivers all training programmes, conducts annual VAPT & STQC audits, manages ISO 27001 certification, and performs AI model retraining bi-annually.

**STAKEHOLDER 3: EXISTING FIELD CONTRACTOR (Technology Service Provider (TSP))**

Companies already appointed by NHAI/IHMCL under separate civil and equipment contracts to install, commission, and maintain the physical ATMS infrastructure on each corridor.

- Installs, commissions, and certifies all field hardware — cameras, gantries, VMS boards, sensors, and ECBs etc. to the standards specified in the TSP contract.
- Maintains and repairs all field hardware under a separate SLA with IHMCL; responds to maintenance tickets automatically raised by the ATMS platform.
- Configures each field device to communicate on the MQTT topic hierarchy and JSON schema specified by the IA in the Device Integration Guide.
- Provides the SDA with a complete device inventory spreadsheet (make, model, serial number, firmware, IP, GPS, KP reference, lane) for population of the asset registry.

- Coordinates with the SDA during LCCC onboarding activities to validate end-to-end data flow from field device through to the national platform.
- Accesses the Contractor Portal, built and hosted by the SDA to view its own SLA performance metrics, device health data, and open maintenance tickets.
- Serves as the first line of defense, enabling immediate response to incidents for timely mitigation and resolution.

### 3.6.3. Step-by-Step Deployment Walkthrough — 6 Stages

The following describes the precise sequence of events for onboarding a 1,200 km corridor onto the National ATMS Platform. Each stage identifies which stakeholder performs which action, and the dependencies between them.

#### STAGE 1 • Site Readiness — IHMCL and Field TSP

<b>IHMCL provides</b>	LCCC buildings across 10–12 locations along the corridor. Each LCCC is fully fitted with stable power supply (UPS and DG backup), precision air conditioning, rack space, and fibre connectivity to the rack. IHMCL issues a formal Site Readiness Certificate (SRC) for each LCCC before the SDA's onboarding clock commences.
<b>IHMCL provides</b>	Infra for ATMS software deployment at LCCC and RCCC.
<b>IHMCL provides</b>	managed MPLS connectivity between NCCC-RCCC-LCCC
<b>Field TSP delivers</b>	All field hardware commissioned and operational — cameras, VMS, sensors, and ECBs etc. across the full 1,200 km. Each device is assigned a fixed IP address, tagged with a kilometre post (KP) reference, and physically cabled to the LCCC
<b>Field TSP delivers</b>	Complete device inventory documentation: make, model, serial number, firmware version, IP address, port number, GPS coordinates, KP reference, and lane number (As applicable). This inventory is formally handed to the SDA for asset registry population and SLA management. The Field TSP shall ensure the accuracy and authenticity of all submitted information. Any discrepancy or submission of false data shall attract stringent penalties over and above contractual penalties as decided and finalized by NHAI/IHMCL.

#### STAGE 2 • Platform Readiness — Software Development Agency

<b>SDA confirms</b>	The national ATMS platform NCCC instances shall be operational on the On-Premise at NCCC supported with MEITY-empanelled cloud service provider for Disaster Recovery. The Production Data Centre (DC) and Disaster Recovery Data Centre (DR), if applicable shall be active-standby with 100% only real time Data. The relevant zonal RCCC shall be commissioned and connected to the NCCC.
<b>SDA deploys</b>	ATMS LCCC Agent software on both edge servers at each of the LCCCs via the SDA's automated CI/CD pipeline. The LCCC Agent package includes: ATMS operations software, AI inference engine (ANPR and VCA models), local DB instance, The Field TSP shall ensure the accuracy and authenticity of all submitted information. Any discrepancy or submission of false data shall attract stringent penalties as per the applicable contract provisions. VMS software, and MQTT broker.
<b>SDA provisions</b>	X.509 device certificates for each LCCC edge server and each field device category, enabling MQTT TLS 1.3 mutual authentication. Certificates are issued via the SDA's centralised PKI/CA system and are configured for automated rotation every 12 months.
<b>SDA configures</b>	The MQTT topic hierarchy for the corridor. Every device is assigned a standardised, hierarchical topic path (e.g., ihmcl/corridor/delhi-mumbai/lcc-05/camera/cam-0423/status).

### STAGE 3 · Device Onboarding — SDA with TSP Coordination

<b>SDA loads</b>	The device inventory received from the TSP into the ATMS Asset Registry. Each camera, sensor, VMS board, and ECB is registered with its KP reference, GPS coordinates, make and model, firmware version, assigned LCCC, and lane number.
<b>SDA configures</b>	ONVIF/RTSP ingestion profiles for every camera in the LCCC Video Management System. Tests live stream ingestion from all cameras. Validates stream quality and end-to-end latency; the specification requires that every stream is visible at the operator console within two seconds.
<b>SDA configures</b>	MQTT subscriptions for all sensor data types — radar speed, weather station telemetry, and ECB call events. Validates message format (JSON schema) and topic routing. Confirms that data flows correctly from the LCCC MQTT broker through to the RCCC and the NCCC Data Lake.
<b>TSP reconfigures</b>	Any devices not transmitting on the correct MQTT topic or with a non-compliant JSON schema, in accordance with the SDA's published Device Integration Guide. The SDA



	provides the TSP with the Device Integration Guide formally at T0+30 days; the TSP is given 60 days to achieve full compliance before the LCCC onboarding milestone date.
<b>SDA validates</b>	End-to-end data pipeline integrity: field device → LCCC MQTT broker → RCCC cluster → NCCC Data Lake. Confirms that live traffic counts, vehicle speeds, and camera feeds are visible on the NCCC GIS dashboard within one second of occurrence at the field device.

#### STAGE 4 · Functional Configuration — SDA with IHMCL Operators

<b>SDA configures</b>	The GIS map layer for the corridor. All 1,200 km are rendered on the national GIS platform with every device icon, kilometre post marker, LCCC boundary, and junction overlay visible and searchable at LCCC, RCCC, and NCCC views.
<b>SDA configures</b>	The Standard Operating Procedure (SOP) library for the corridor. Minimum mandatory SOPs: accident response, wrong-way vehicle alert, congestion threshold trigger, weather advisory, road closure, and VMS cascade. Each SOP specifies automated actions — dispatch, VMS update, notification escalation — and defined human approval gates.
<b>SDA configures</b>	Enforcement rules: speed limits per highway segment, enforcement camera KP references, ANPR station pairing for journey time computation, and watch-list query routing to the nearest operational LCCC.
<b>IHMCL approves</b>	All SOPs, enforcement rules, and VMS message templates through the ATMS platform's formal approval workflow before the corridor goes live. No enforcement or automated VMS commands are activated without IHMCL's signed approval.
<b>SDA delivers</b>	LCCC operator training (Modules TRN-01 through TRN-08) for all operators at the LCCCs on this corridor. Training is conducted using the dedicated training environment loaded with Delhi–Mumbai corridor scenario scripts. Operators must achieve certification before the corridor goes into live operations.

#### STAGE 5 · Site Acceptance Testing — All STAKEHOLDERS

<b>IHMCL leads</b>	SDA shall provide a detailed SAT document for each module and shall get it approved from NHAI/IHMCL. The SDA submits the SAT plan for IHMCL approval at least four weeks before testing commences. Test cases cover: all devices visible on GIS; e-challan generated end-to-end from respective LCCC; incident SOP executed end-to-end; VMS commands
--------------------	--



	dispatched and acknowledged; LCCC autonomous operation validated over 72 hours of simulated WAN outage.
<b>SDA executes</b>	All test cases, documents result in the Acceptance Test Report and remediates defects. All Critical and High severity defects must be formally closed before SAT sign-off can be granted. Medium severity defects may be conditionally accepted with a contractually binding closure date not exceeding 30 days post-SAT.
<b>Field TSP participates</b>	To validate that all field devices respond correctly to software commands — VMS message display, camera PTZ commands, ECB call routing etc. and that device health telemetry is being accurately reported to the platform in real time.
<b>IHMCL issues</b>	The SAT Completion Certificate for the corridor upon satisfactory completion of all acceptance criteria for each module. From the date of this certificate, the SLA performance clock commences for both the SDA (software platform SLA) and the TSP (field hardware SLA).

#### 3.6.4. Consolidated Responsibility Matrix

The matrix below provides the definitive single-page reference for accountability and execution responsibilities across every key activity in the 1,200 km corridor deployment and subsequent ongoing operations. Designations: R = Responsible (executes the work), A = Accountable (signs off and is ultimately liable), C= Consulted, S = Supports, N/I = Not Involved.

Activity / Asset	IHMCL / NHAI	SDA (Software Vendor)	Field TSP / Contractor
<b>HARDWARE &amp; INFRASTRUCTURE</b>			
<b>Camera, VMS &amp; sensor procurement</b>	Accountable — funds and procures under TSP contract	Not Involved	Responsible — supplies, installs, and commissions
<b>LCCC building, power supply &amp; rack fit-out</b>	Responsible — provides building, power, A/C, and rack	Supports — specifies server rack requirements	Supports — field cable termination
<b>Edge servers (hardware) at each LCCC</b>	Responsible — procures hardware per IA specification	Not Involved	Responsible — supplies, installs, and commissions
<b>Managed MPLS connectivity LCCC↔RCCC↔NCCC</b>	Accountable — orders, funds, and owns all circuits	Not Involved	Responsible — supplies, installs, and commissions

Activity / Asset	IHMCL / NHAI	SDA (Software Vendor)	Field TSP / Contractor
<b>SOFTWARE PLATFORM</b>			
<b>NCCC / RCCC cloud platform (software)</b>	Consulted	Responsible — builds, deploys, and operates 24×7	Not Involved
<b>LCCC Agent software deployment</b>	Consulted	Responsible — remote deployment via CI/CD pipeline	Not Involved
<b>AI models (ANPR, VCA, behavioural)</b>	Consulted	Responsible — trains, deploys, and retrains bi-annually	Supports — camera field calibration
<b>MQTT broker &amp; device onboarding pipeline</b>	Consulted	Responsible — configures per corridor	Supports — reconfigures devices to match SDA spec
<b>Open-Source GIS deployment, Customization and Integration with sensors and third-party National GIS platforms (PM Gati Shakti etc.)</b>	Consulted	Responsible — configures per corridor	Supports — Integration of field and control room infra with SDA ATMS platform.
<b>Generation of e-challan from RCCC</b>	Consulted	Responsible — Integrates the violation data from each LCCC and generates e-challan with NIC for each region.	Supports — Provides true audited data with necessary evidence for generation of e-challan to RCCC.
<b>Real time health monitoring, SLA &amp; asset management engine</b>	Consulted	Responsible — builds; IHMCL uses as governance tool	Supports — Provides Mac address, Ip address etc. for real time health monitoring and integration of field and control room infra

Activity / Asset	IHMCL / NHAI	SDA (Software Vendor)	Field TSP / Contractor
			with local, regional and national EMS/NMS.
<b>GOVERNMENT API INTEGRATIONS</b>			
<b>API access credentials (VAHAN, FASTag, etc.)</b>	Responsible — obtains approval/support from respective ministries for integration	Supports — integration design	Consulted
<b>VAHAN / SARATHI integration development</b>	Accountable — signs MoU with MoRTH / NIC	Responsible — develops, tests, and maintains	Consulted
<b>FASTag / NETC integration</b>	Accountable — IHMCL owns FASTag programme	Responsible — integrates into ANPR workflow	Consulted
<b>Police e-challan system integration</b>	Accountable — signs MoU with State Police/MHA	Responsible — develops challan dispatch pipeline	Consulted
<b>COMPREHENSIVE OPERATIONS &amp; MAINTENANCE</b>			
<b>24×7 NCCC operations</b>	Accountable — IHMCL-employed operators	Responsible — platform support and training	Not Involved
<b>Platform software NOC (cloud + LCCC agent)</b>	Consulted	Responsible — 24×7 SDA NOC team	Not Involved
<b>Field hardware fault repair</b>	Accountable	Not Involved	Responsible — within contracted SLA times
<b>Annual VAPT &amp; STQC (cybersecurity)</b>	Accountable — reviews findings report	Responsible — engages CERT-In empanelled firm	Not Involved
<b>CYBERSECURITY &amp; COMPLIANCE</b>			

Activity / Asset	IHMCL / NHAI	SDA (Software Vendor)	Field TSP / Contractor
<b>NCIIPC CII registration</b>	Accountable — approves and files	Responsible — prepares documentation	Not Involved
<b>ISO 27001:2022 certification</b>	Accountable — required as contract condition	Responsible — achieves and maintains	Not Involved
<b>CERT-In incident reporting (6-hour)</b>	Consulted	Responsible — CSOC operation 24×7	Not Involved

#### 4. NATIONAL ATMS OPERATIONAL CONCEPT

The National ATMS Operational Concept defines the manner in which the system will be operated, the roles of stakeholders at each level of the command hierarchy, the information flows between systems, and the operational scenarios that the system must support.

##### 4.1. System Purpose and Vision

The National ATMS is conceived as a multi-tier intelligent traffic management platform that transforms India's national highway network into a digitally managed corridor system. Unlike conventional highway management systems that operate in isolation at individual toll plazas or project stretches, the National ATMS provides a unified fully integrated operational picture from a single national command centre while simultaneously enabling autonomous, resilient operations at regional and local levels. It will be built like a Digital Public Infrastructure.

##### 4.2. Key Stakeholders

Stakeholder	Role and Responsibilities
<b>Ministry of Road Transport &amp; Highways (MoRTH)</b>	Policy oversight, national performance review, inter-ministry coordination

<b>National Highways Authority of India (NHAI)</b>	System ownership, national operations, SLA governance, contractor oversight
<b>Indian Highway Management Company Ltd (IHMCL)</b>	FASTag programme, commercial operations, toll enforcement integration
<b>National ATMS Command and control centre (NCCC)</b>	24x7 national operational control, national incident management, cross-corridor coordination, decision support systems and drilldown visibility
<b>Regional Command and control Centres (RCCC)</b>	Regional operations across 5 zones: North, South, East, West, Central
<b>Local Command and Control Centres (LCCC)</b>	Project-level operations, field device management, local data processing, first-response coordination
<b>Traffic Police (State / NH Police)</b>	Enforcement actions, patrol deployment, FIR registration for accidents, E-challan issuance
<b>National Highways &amp; Infrastructure Dev. Corp (NHIDCL)</b>	North and North-East corridor operations
<b>State Road Transport Authorities</b>	State ICCC integration, state-level policy alignment
<b>Emergency Services (NHAI Ambulance, NDRF)</b>	Emergency response coordination, accident site management
<b>Technology Service Providers (TSPs)</b>	Comprehensive System O&M, field maintenance, SLA adherence
<b>Road Users</b>	Beneficiaries of the system; and traffic data

### 4.3. Operational Scenarios

#### 4.3.1. Normal Operations

Under normal operating conditions, the local ATMS software (at LCCC) continuously ingests data from all connected field devices including TMCS/CCTV cameras, VIDEs and ANPR cameras, radar sensors, Meteorological Sensors, and Variable message Signboard units. The system performs real-time stream processing of all data, applies AI-based analytics to detect anomalies, and maintains a live operational dashboard for all command centre levels. Traffic classification, counts, speeds, occupancy, and weather data are logged to the national data lake with full time-series history.

VMS messages are updated automatically at local / edge levels based on predefined rules and real-time traffic conditions. Traffic management plans are executed automatically for known recurring congestion patterns (school hours, weekends, festival seasons) and manually triggered by operators for special events. RCCCs and NCCC shall

have full control of all the messages to be scheduled as per requirements and this shall be pushed to respective board and message priority shall be clearly defined for each level to remove ambiguity.

#### **4.3.2. Incident Response Operations**

When an incident is detected locally either through automatic video incident detection, manual CCTV observation, or a report from a road user or patrol: the system executes the National Incident Response Protocol. The incident is classified by type (accident, breakdown, debris, wrong-way driving, fire, flooding as defined) and severity (minor, moderate, major, catastrophic). Based on classification and severity, the system automatically dispatches notifications to the appropriate response resources (ambulance, patrol vehicle, recovery vehicle), updates VMS messages upstream of the incident, and generates an incident report which can be catered at LCCC and informed / escalated appropriately at NCCC and RCCC.

The incident management workflow tracks the response timeline from detection through attendance, clearance, and post-incident review. All timestamps are recorded and compared against Service Level Agreement targets. Incidents that breach SLA thresholds trigger automatic escalation to the next command level.

#### **4.3.3. Enforcement Operations**

Enforcement operations are triggered when the Existing Field Platform Vendor's enforcement module detects a traffic violation and transmits a structured violation event to the ATMS Platform. The ATMS Platform receives the violation record (including ANPR plate read, vehicle class, evidence reference, and violation type), queries VAHAN for registered owner details if required, and provides the enforcement data to the reporting and analytics modules. e-Challan generation, evidence capture, and direct NIC portal transmission are performed by the Vendor enforcement module. The ATMS Platform collects violation information from existing system and challan metadata stages (generated, notified etc.) via the e-Challan data feed and provides enforcement analytics to IHMCL and NHAI leadership dashboards.

#### **4.3.4. Severe Weather and Disaster Operations**

The system integrates real-time weather data from meteorological sensors and the Indian Meteorological Department (IMD) API. When weather conditions deteriorate beyond defined thresholds (wind speed, visibility, rainfall, fog density) and verified by the operators, the system automatically triggers weather-based speed limit reductions, preventive messages through VMS updates and notifies road users and local staff. For severe events such as cyclones, flooding, or landslides, the system activates the Disaster Response Protocol, which may include road closures, traffic diversion, and coordination with NDRF and State Disaster Management Authorities (SDMAs). Platform software shall also have a feature to integrate with social media platforms, News platforms etc. for taking real time inputs and updates.

#### **4.3.5. Cyber Incident Response**

The ATMS Cybersecurity Operations Centre (CSOC), integrated with the national SIEM platform, operates 24x7 to monitor for cyber threats. Upon detection of a cyber incident, the Cyber Incident Response Plan is activated. Depending on severity, this may involve isolating affected network segments, revoking compromised credentials,

---

rolling back affected configurations, and reporting to CERT-In within the mandated timeframe. All cyber incidents are documented and subject to post-incident review.



## 5. NATIONAL – REGIONAL – LOCAL COMMAND AND CONTROL CENTRE HIERARCHY

The National ATMS operates within a three-tier command hierarchy that mirrors the administrative structure of NHAIT and reflects the geographic and functional distribution of operations across India's national highway network.

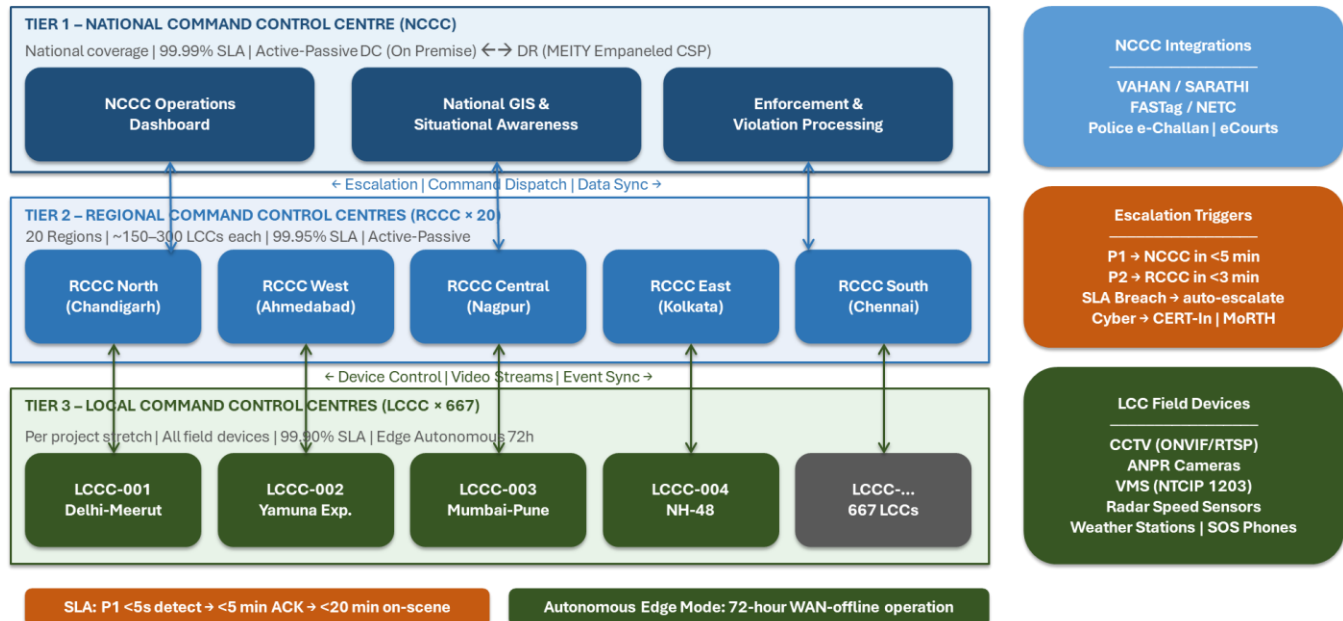


Figure 4: Three Level Command Hierarchy

### 5.1. National Command and Control Centre (NCCC)

The National Command Centre is the apex command authority for the national ATMS. Located at NHAIT Headquarters in New Delhi, the NCCC operates 24 hours a day, 365 days a year. This shall be deployed with on premises infra (Videowall, Server, SAN Storage, Workstations, Networking infra etc., however this infra shall be provided by IHMCL and procurement of On premises NCCC infra is not in scope of SDA). The NCCC provides a unified national operational picture, exercises authority over all national-level incidents and decisions, and serves as the primary interface with MoRTH, IHMCL, and inter-ministry coordination forums.

#### 5.1.1. NCCC Functional Responsibilities

- Maintain the national situational awareness dashboard with real-time status of all highway corridors, major incidents, and system performance.
- Exercise supervisory authority over all Regional Command Centres.
- Manage national-level incidents (catastrophic, cross-regional, or involving fatalities).
- Coordinate with emergency services, police, NDRF, and State governments for major incidents.
- Monitor national SLA compliance for all ATMS TSPs.
- Provide national traffic data to MoRTH, IMD, and other authorised agencies.
- Manage the national enforcement database and coordinate with IHMCL for FASTag-linked penalties.

NATIONAL SITUATIONAL AWARENESS & COMMAND	ANALYTICS, REPORTING & LEADERSHIP DASHBOARDS	SECURITY, COMPLIANCE & DATA GOVERNANCE
<b>1</b> National GIS dashboard — all 20+ RCC regions with real-time aggregate metrics: active incidents, device health %, violation counts, weather alerts per region FRS: FR-GUI-NCC-001, FR-HTM GIS VDIL EPE DL	<b>1</b> MoRTH/NHAI leadership dashboards — programme KPIs: incident rate trend, SLA compliance, enforcement revenue (from vendor feed), system availability FRS: FR-GUI-NCC-002, FR-RPT-004 RPT DL VDIL	<b>1</b> 24x7 CSOC — monitor SIEM for cyber threats; UEBA anomaly detection; CERT-In incident reporting within 6 hours of detection FRS: FR-SEC-005..009 SIEM IAM EPE
<b>2</b> Cross-regional incident escalation — receive Major/Catastrophic from RCC; initiate national response including DMC/SDMA notification within 2 minutes FRS: FR-GUI-NCC-003, FR-COM-009 IPE CDE VDIL	<b>2</b> AI predictive analytics — congestion forecasts (1hr+4hr, ≥80% accuracy); incident risk heatmap; device failure predictions FRS: FR-DAT-004..007 DL RPT GIS	<b>2</b> API Gateway security oversight — OAuth 2.0 / mTLS token management; rate limiting; API transaction audit for all 19 integrations FRS: FR-COM-003, FR-INT-023 IAM VDIL SIEM
<b>3</b> National broadcast VMS advisory to multiple regions simultaneously — request dispatched to vendor VASD APIs across all corridors FRS: FR-GUI-NCC-003, FR-INT-019 CDE VDIL	<b>3</b> Annual programme performance report for MoRTH/NHAI — safety improvements, SLA trends, enforcement revenue YTD, platform availability FRS: FR-RPT-004, FR-RPT-015 RPT DL	<b>3</b> Annual DR test oversight — full DC1→DR1 failover simulation; RTO<4 hours, RPO<1 hour; IHMCL sign-off; test report FRS: FR-SYS-006 NMS SIEM IAM
<b>4</b> Monitor all 19 external government API integrations — VAHAN, SARATHI, FASTag, CCTNS, iCAD health dashboard FRS: FR-INT-001..023, FR-COM-011 VDIL NMS ALM	<b>4</b> KPI Framework — national programme KPI dashboard with configurable RAG indicators; NHAI ATMS Policy Chapter 7 compliance report monthly FRS: FR-RPT-001..005, FR-KPI RPT DL GIS	<b>4</b> Cloud infrastructure capacity management — annual capacity review; scaling plan approved by IHMCL; cloud cost optimisation reports quarterly FRS: FR-SYS-004..007 NMS DL
<b>5</b> Access multi-source intelligence dashboard — social media NLP signals, crowd reports correlated with ITS data across national network FRS: FR-SRC-001..008 EPE DL VDIL	<b>5</b> End-of-day automated push of all ATMS operational data to NHAI DataLake/ERP via API FRS: FR-RPT-015, FR-INT RPT DL VDIL	<b>5</b> State ICCC bi-directional event sharing (DATEX II v3.2); Police PCR dedicated feed management (MPLS/OFC); DMC/SDMA NDMA schema push FRS: FR-COM-007..010, FR-INT-013 VDIL CDE IAM

Figure 5: NCCC Functional Use Cases

## 5.2. Regional Command and control Centres (RCCC)

Regional Command Centres shall be established covering the following zones: North Zone (Delhi, Haryana, Rajasthan, HP, J&K, Punjab), South Zone (Tamil Nadu, Karnataka, Kerala, Andhra Pradesh, Telangana), East Zone (West Bengal, Odisha, Bihar, Jharkhand, North-East States), West Zone (Maharashtra, Gujarat, Goa), and Central Zone (Madhya Pradesh, Chhattisgarh, Uttar Pradesh, Uttarakhand).

Each RCCC exercises command authority over all LCCCs and TSPs within its zone. RCCCs manage regional incidents, coordinate cross-project operations, and provide the NCCC with aggregated zone-level situational awareness reports every 15 minutes under normal operations and in real-time during declared incidents.

REGIONAL SITUATIONAL AWARENESS	INCIDENT ESCALATION & CROSS-LCC COORDINATION	REPORTING, GOVERNANCE & SLA MANAGEMENT
<b>1</b> Regional GIS map — all LCC corridors in zone with live incident icons, traffic speed (from vendor ATCC/VIDS), device health, weather overlays FRS: FR-GUI-RCC-001, FR-HTM GIS VDI L EPE	<b>1</b> Receive auto-escalation for Moderate+ incidents from any LCC in region (<60 sec); RCC supervisor assigned automatically FRS: FR-INCD-008, FR-INCD-015 IPE ALM	<b>1</b> Regional weekly/monthly SLA performance reports — auto-generated; TSP penalty computation; Contractor Portal visibility FRS: FR-NMS-011..015, FR-RPT-007 NMS RPT VDI L
<b>2</b> Inter-corridor traffic comparison dashboard — congestion correlation, incident frequency, weather impact across region FRS: FR-GUI-RCC-003, FR-DAT GIS DL RPT	<b>2</b> Assume supervisory control of an LCC in emergency — view LCC console, approve SOP tasks, override decisions FRS: FR-GUI-RCC-002 IPE GIS IAM	<b>2</b> Approve or request VMS advisory campaigns covering multiple corridors — request forwarded to vendor VASD API FRS: FR-COM-002, FR-INT-019 CDE VDI L
<b>3</b> Device availability heatmap — ATMS and vendor devices across all TSPs in region; SLA compliance at a glance FRS: FR-NMS-009, FR-SLA NMS VDI L RPT	<b>3</b> One-click escalation of Major incidents to NCC — auto-populated summary, mandatory justification captured FRS: FR-GUI-RCC-004 IPE CDE RPT	<b>3</b> Monitor maintenance ticket queue for all TSPs in region — SLA reminder alerts at 80% and 100% elapsed time FRS: FR-NMS-016..019 NMS ALM
<b>4</b> Monitor vendor VDI L feed health — VIDES, ANPR, VMS, e-Challan, ATCC feeds across all LCCs in region FRS: FR-INT-016..021 VDI L NMS ALM	<b>4</b> Coordinate multi-agency SOP tasks across LCC and agency boundaries — police, ambulance, NHAI patrol simultaneously FRS: FR-INCD-016, FR-SOP-002 IPE AUD CDE	<b>4</b> Access PIU/RO read-only portal access for NHAI Project Implementation Units within the region FRS: FR-COM-005..006 RPT IAM
<b>5</b> Receive multi-source intelligence dashboard — social media signals, crowd reports, correlation with ITS sensor data FRS: FR-SRC-001..004 EPE DL ALM	<b>5</b> View enforcement analytics from vendor e-Challan feed — regional violation statistics, repeat offender patterns FRS: FR-RPT-006, FR-INT-020 VDI L RPT DL	<b>5</b> Generate weekly enforcement revenue reports (from vendor e-Challan feed) for IHMCL regional management FRS: FR-RPT-006, FR-DAT-007 VDI L RPT DL

Figure 6: RCCC Functional Use Cases

### 5.3. Local Command and Control Centres (LCCC)

Local Control Centers are deployed at each ATMS project stretch, typically located at the primary toll plaza or the mid-point of the project. Each LCCC manages all field devices within its project boundary, handles routine incident response for minor and moderate incidents, manages day-to-day device maintenance coordination with TSPs, and provides 24x7 monitoring of local CCTV and sensor feeds.

The LCCC operates on edge computing infrastructure that provides full autonomous operational capability in the event of connectivity loss to the RCCC or NCCC. Local incident management, VMS control, and device monitoring continues uninterrupted during communication outages. All locally buffered data is synchronized to the RCCC/NCCC upon restoration of connectivity.

CORRIDOR MONITORING & SITUATIONAL AWARENESS	INCIDENT MANAGEMENT & SOP EXECUTION	COMMUNICATIONS, ENFORCEMENT & MAINTENANCE
<b>1</b> Monitor live GIS map — all field devices, active incidents, traffic speed, weather, patrol vehicle GPS FRS: FR-HTM-001..014 GIS EPE NMS	<b>1</b> Receive structured incident detection event from vendor VIDES feed (<5 sec). Confirm or reject with one click — rejection logged for vendor AI feedback FRS: FR-INCD-001..006 IPE VDIL EPE	<b>1</b> Manage 1033/ECB calls — integrated audio; all calls recorded, WORM stored, tamper-proof FRS: FR-AUD-001..006 AUD DCE
<b>2</b> View CCTV stream tokens on video wall (up to 16 streams — from vendor TMCS via ATMS gateway) FRS: FR-GUI-LCC-002 GIS VDIL	<b>2</b> Execute auto-assigned SOP tasks: call ambulance/police/crane via Integrated Audio (context-sensitive SOP dial) FRS: FR-SOP-001..011, FR-AUD IPE AUD CDE	<b>2</b> Review enforcement records from vendor e-Challan feed — view violation data, challan lifecycle status FRS: FR-INT-020, FR-RPT-006 VDIL RPT
<b>3</b> Receive real-time alarm notifications — device faults, incident detections, SLA breaches, weather threshold alerts FRS: FR-ALM-001..005 ALM EPE	<b>3</b> Dispatch emergency vehicles via 1033 iCAD — track response in real time on GIS map (AIS-140 GPS) FRS: FR-INT-010, FR-HTM-013 CDE GIS IPE	<b>3</b> Raise and track maintenance tickets for faulty devices — update via Mobile App in field FRS: FR-NMS-016..019 NMS MOB
<b>4</b> Monitor VMS advisory status — current message on each sign, device health (from vendor VASD feed) FRS: FR-HTM-006, FR-NMS GIS VDIL NMS	<b>4</b> Request VMS advisory message for upstream signs (request sent to vendor VASD API via CDE) FRS: FR-SOP-009, FR-INT-019 CDE VDIL	<b>4</b> Access shift handover report — view open incidents, device faults, pending SOP tasks from previous shift FRS: FR-RPT-010 RPT IPE
<b>5</b> Strip chart corridor view — linear KP-by-KP device and incident status FRS: FR-GUI-LCC-005 GIS	<b>5</b> Close incident — mandatory SOP completion check; post-incident report auto-generated FRS: FR-INCD-019..020 IPE RPT	<b>5</b> Operate in autonomous mode (WAN loss) — all local functions preserved 72 hrs; auto-sync on reconnect FRS: FR-GUI-LCC-004, FR-SYS-006 EPE IPE GIS

Figure 7: LCCC Functional Use Cases

#### 5.4. Operational Architecture

The Local Command & control Centre (LCCC) serves as the tactical frontline, focusing on real-time corridor monitoring, immediate incident response, managing emergency calls, and dispatching field support. Moving up, the Regional Command & control Centre (RCCC) provides broader oversight by monitoring multiple LCCCs simultaneously, managing cross-corridor traffic patterns, coordinating multi-agency responses, and tracking regional performance SLAs. At the apex, the National Command & control Centre (NCCC) handles strategic nationwide operations, including cross-regional escalations, managing national API gateways (such as VAHAN and FASTag), overseeing cybersecurity, and utilizing AI for predictive analytics and high-level leadership reporting.



Figure 8: Three Tier Operational Function Overview

### 5.5. Incident Monitoring Authority Matrix

Incident / Action Type	NCCC Authority	RCCC Authority	LCCC Authority
Minor Incident (no injury)	Monitor	Monitor	Manage & Resolve
Moderate Incident (injury)	Monitor & Support	Manage & Resolve	First Response
Major Incident (fatality)	Manage & Resolve	Coordinate & Support	First Response
Cross-Regional Incident	Manage & Resolve	Coordinate	Support
Cyber Incident	Lead Response	Support	Report
VMS Message Approval	National Campaigns	Regional Campaigns	Local & Routine
SLA Dispute Resolution	Final Authority	Initial Review & report	Data Provider
Road Closure (full)	Approve	Recommend	Propose
Weather Advisory	National Advisories	Regional Advisories	Local Advisories

## 6. OVERALL SYSTEM ARCHITECTURE

The National ATMS employs a hybrid cloud-edge architecture that combines the scalability and processing power of a national cloud platform with the low-latency, autonomous capabilities of edge computing at local control centres. This architecture is designed to meet the stringent availability, performance, and scalability requirements of a mission-critical national infrastructure system. The broad architecture is as below:

The on-premise infrastructure shall be provided by the respective Zonal ATMS Field System Integrator for LCCCs, RCCCs and NCCC, while the cloud infrastructure for Disaster Recovery (DR) shall be provisioned and managed by the IHMCL for NCCCs.

The hosting & storage architecture of the Unified ATMS Software shall follow a distributed hybrid infrastructure model, balancing on-premises operational resilience with the scalability and elasticity of resources across the three-tier Command Centre framework comprising of LCCCs, RCCCs, and the NCCC as below:

### a) Hosting of the Unified ATMS Software:

CCC tier	On-premise Infra	Cloud Infra (DR)
Local CCC	Yes	Not Required
Regional CCC	Yes	Not Required
National CCC	Yes	Yes (Control Only)

### b) Storage requirement of the Unified ATMS Software:

CCC tier	On-premise Infra	Cloud Infra Requirement
Local CCC	Yes	Not Required
Regional CCC	Yes	Not Required
National CCC	Yes	Only Real Time Data (No DC Sync)

### 6.1. Architecture Principles

- **Cloud-Native Design:** All components at the NCCC and LCCC, RCCC levels are designed as cloud-native microservices, enabling independent scaling, rolling updates, and high availability. The NCCC shall be deployed on premise with DR on cloud infrastructure, whereas the RCCCs and LCCCs platforms shall be deployed on-premises only. However, the platform at each tier shall be designed to be cloud-ready.
- **Edge Autonomy:** LCCC edge nodes operate fully autonomously during connectivity loss, ensuring uninterrupted local operations.
- **Active-Passive Redundancy:** NCCC shall be deployed in Active Standby with RTO and RPO of 2 and 4 HRS respectively.
- **Zero Trust Security:** All inter-component communication is authenticated and encrypted, with no implicit trust granted based on network location.

- **API-First Integration:** All system interfaces are exposed through the National API Gateway using standardised RESTful or MQTT protocols.
- **Data Sovereignty:** All data is stored in MEITY-empanelled cloud infrastructure within Indian territory, compliant with data localisation requirements.
- **Vendor Neutrality:** The architecture is designed around open standards to avoid vendor lock-in and enable competitive procurement.
- **Standardised Hardware Communication Protocol:** All field edge devices SHALL communicate using MQTT v5.0 over TLS 1.3, port 8883. Standardised topic naming and JSON message envelopes enable any certified hardware vendor's equipment to integrate seamlessly, preserving vendor independence at the edge layer.

## 6.2. National Command and Control Centre (NCCC) Architecture

The National Command Centre operates on On-premise Infrastructure at local data centre hosted at NCCC with geographically separated disaster recovery site. The cloud platform for Disaster Recovery to be built on MEITY-empanelled infrastructure and supports both government cloud (MeghRaj) and certified private cloud deployments having 100% compute of the actual requirement at Data Centre with real time data as per the latest relevant cloud policy.

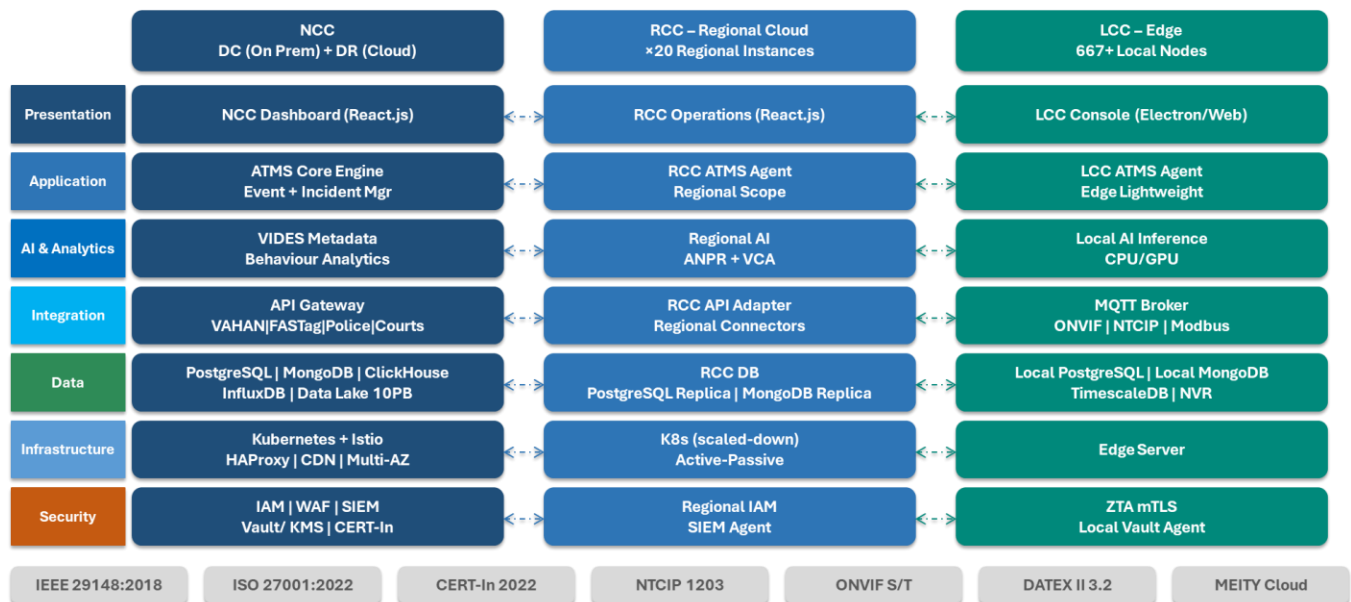


Figure 9: Representation of Enterprise Software Architecture - Layered View

### 6.2.1. NCCC Infrastructure Stack

Layer	Component	Technology / Standard
Presentation	National Operations Dashboard, GIS Viewer, Management Portals	React.js/ Angular, Leaflet/ OpenLayers GIS, WebSocket



Application	ATMS Core Engine, AI Processing, API Gateway, Notification Services	Java Spring Boot, Python (AI/ML), Pytorch/ Tensorflow, Node.js, Apache Kafka
Integration	ESB / Integration Bus, VAHAN/SARATHI connectors, FASTag adapter and other DBs.	Apache Camel, REST/SOAP, MQTT, JSON, DATEX II
Data	Operational DB, Data Warehouse, Time-Series DB, Message Queue	PostgreSQL, MongoDB, ClickHouse, InfluxDB, Apache Kafka, S3/ Cloudflare R2/ Minio
API	API Gateway	Kong, Zuul
Infrastructure	Container Orchestration, Service Mesh, Load Balancing, CDN	Kubernetes, Istio, HAProxy/NGINX, Cloudflare, Akamai
Security	IAM, WAF, Secrets Management, SIEM, Vulnerability Scanner	HashiCorp Vault, KMS, OAuth, OWASP ZAP, Splunk/ELK, CrowdStrike
Monitoring	APM, Infrastructure Monitoring, Log Aggregation, Alerting	Prometheus/Grafana, ELK Stack, PagerDuty

The specific technology stacks mentioned in the diagram are indicative. SDA is expected to propose their own stack with specific preference for opensource technologies and tools, with no proprietary lock-ins.

### 6.3. Regional Command and Control Centre (RCCC) Architecture

Regional Command Control Centres operates on dedicated on-premises infrastructure, deployed in HA configuration with automatic failover.

RCCC infrastructure is sized to handle all field devices and data streams within the region autonomously, without dependency on the NCCC. The RCCC maintains a local operational database replica synchronised with the NCCC. In the event of connectivity loss to the NCCC, the RCCC continues full operations and queues differential data for synchronisation upon reconnection.

### 6.4. Local/Edge Command and Control Centre (LCCC) Architecture

Local Control Centre edge nodes are deployed as ruggedised computing units within the LCCC building or independent cloud instances (To be implemented in future) at each ATMS project. The edge architecture is designed to provide full autonomous operation for a minimum of 168 hours in the event of complete connectivity loss to the RCCC.

---

**6.4.1. LCCC Edge Hardware (NOT IN SCOPE OF SDA)**

**Highway Gantry Deployment Specification:** ATMS gantry units shall be deployed at intervals of 5 to 10 km along national highways in line with the latest ATMS policy. Each gantry shall be equipped with the following complied and certified hardware components:

- Speed Detection Sensors: Radar sensors monitoring vehicle speeds per lane and detecting over-speed violations.
- AI-Enabled ANPR Cameras: Minimum 95% OCR accuracy (Day and Night for HSRP) for licence plate capture, for real-time recognition.
- AI Video Analytics Cameras: Detect accidents, stopped vehicles, wrong-way driving, congestion and other incident as defined in the latest ATMS policy.
- Meteorological and Environmental Sensors: Monitor temperature, visibility, precipitation, and wind speed for road condition assessment.
- Edge Controller: Local processing unit with MQTT broker, edge analytics, and minimum 72-hour event buffering for connectivity outage resilience.
- Primary Server: 2x 16C Intel Xeon server with minimum 128GB RAM, 4TB NVMe SSD storage, GPU for AI as required.
- Secondary Server: Hot standby with automatic failover.
- Edge Switch: Layer 2 managed switch for all field device connectivity.
- UPS / Generator: Minimum 4 hours UPS autonomy with generator backup.
- VMS Server: As per site requirements
- Firewall: As per site requirements.

**6.4.2. Infrastructure**

All infrastructure required for e-challan issuance, including speed enforcement systems, shall be duly calibrated and certified in accordance with applicable government policies on an annual basis. The TSP shall ensure full compliance with this requirement, and any challenges or disputes raised by end users in this regard shall be addressed and resolved by the TSPLCCC Edge Software

- ATMS LCCC Agent: Lightweight ATMS operations software with full device management, incident management, and GIS capabilities.
- AI Inference Engine: Local AI models for ANPR, video incident detection, and behaviour analysis.
- Local Operational DB: PostgreSQL/Similar with time-series extension, replicated to RCCC/NCCC when connectivity is available.
- Video Management System (VMS-S): Local video management with ONVIF integration, recording, and RTSP streaming.
- MQTT Broker: Local device communication broker for sub-second device command dispatch.

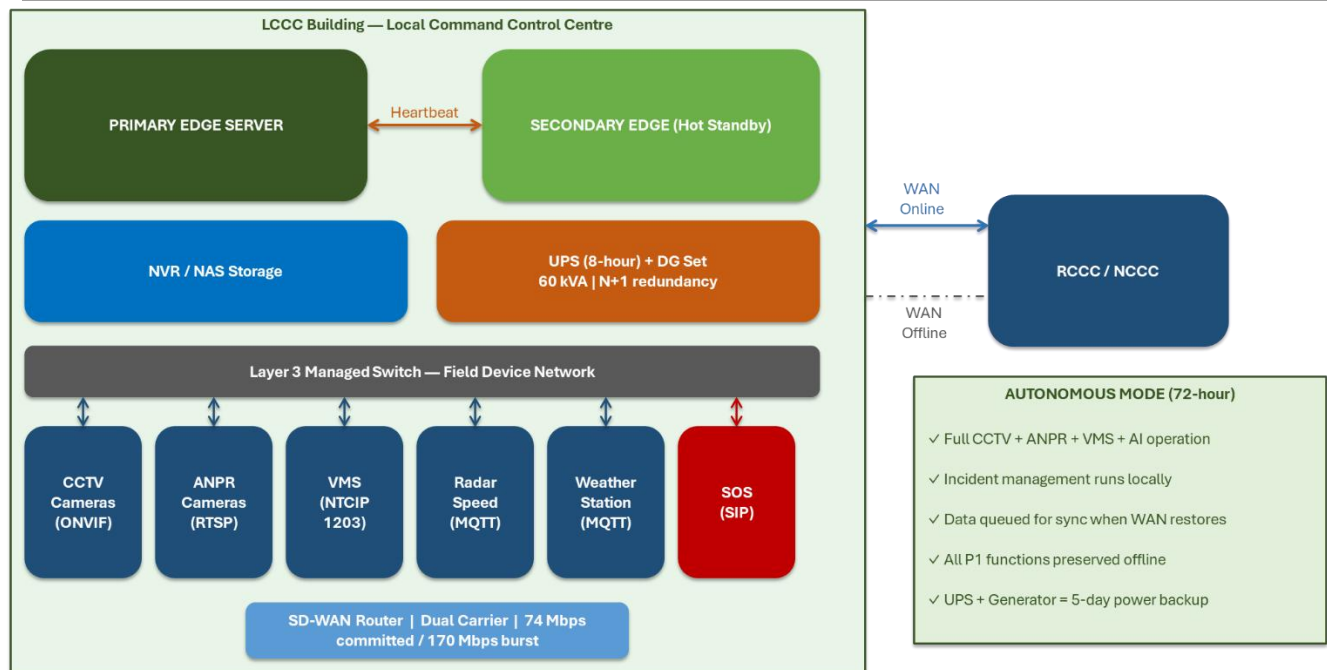


Figure 10: LCCC Edge Architecture &amp; Autonomous Operation Mode

## 7. DETAILED ATMS SOFTWARE STACK

### 7.1. CORE ATMS PROCESSING ENGINE

#### CORE PROCESSING ENGINES

Event Processing Engine (EPE)	Incident Processing Engine (IPE)	Device Communication Engine (DCE)	Command Dispatch Engine (CDE)	Real-Time Stream Processing Layer
Apache Kafka + Flink 100K events/sec Schema validation Data enrichment Event correlation Topic routing	Full lifecycle manager Detected → Closed SOP orchestration SLA timer tracking Multi-tier escalation ICAD dispatch	MQTT v5.0   SNMP SIP/VoIP (ECB/1033) REST/HTTPS X.509 cert lifecycle Bidirectional comms Heartbeat monitor	Priority queue VMS advisory → VASD PTZ advisory → TMCS ICAD dispatch NERS 112 notify Audit log all cmds	Kafka-backed Flink/Spark jobs Containerised K8s Declarative DSL Zero-downtime updates Auto-scale HPA

#### SUPPORTING PLATFORM COMPONENTS

Unified National GIS Platform	National API Gateway	National Data Lake (3-Zone)	Cybersecurity Stack	Governance & Monitoring Platform
PostGIS/PostgreSQL GeoServer tile server 18 configurable layers Real-time COP Historical replay PM Gati Shakti	Kong / Zuul / Other OAuth 2.0 + mTLS 19 Gov integrations VDIL vendor feeds Rate limiting Audit logging	Bronze/Silver/Gold Apache Parquet Delta Lake format 2PB→50PB Y1→Y10 Auto lifecycle mgmt Data lineage	ZTA   MFA   SIEM EDR   PAM   IDS/IPS AES-256 / TLS 1.3 CERT-In compliant NCIIPC CII ISO 27001:2022	Grafana/Prometheus/ ELK Distributed tracing APM dashboards KPI engine Report scheduler SLA dashboard

Figure 11: ATMS Software Stack with Core Processing Engines

### WORK PACKAGE 1: CORE PLATFORM ARCHITECTURE & DEVELOPMENT (Years 1–5).

This section covers the design, development, testing, stabilization, and ongoing product governance of the Unified National ATMS Software Platform during the first five years of the contract. It includes all platform modules, DevOps infrastructure, observability frameworks, cybersecurity, and program management

The ATMS Processing Engine is the central computational core of the National ATMS software platform. It comprises five tightly integrated processing modules collectively handling real-time data ingestion, event processing, incident lifecycle management, device communication, and command dispatch across all three tiers (NCCC, RCCC, LCCC). Maps to FRS Modules: DAQ (Data Acquisition), INCD (Incident Management), and supports all other modules.

#### 7.1.1. Event Processing Engine (EPE)

The EPE is a distributed stream processing system built on Apache Kafka (message backbone) and Apache Flink or Apache Spark Structured Streaming (stateful processing). It receives all raw data streams — from ATMS-managed field devices (TMCS, VIDES< ANPR, VASD, ECBs, network equipment etc.) and structured event feeds from the

Existing Field Platform Vendor — and applies real-time processing rules to classify, enrich, correlate, and route events to downstream modules.

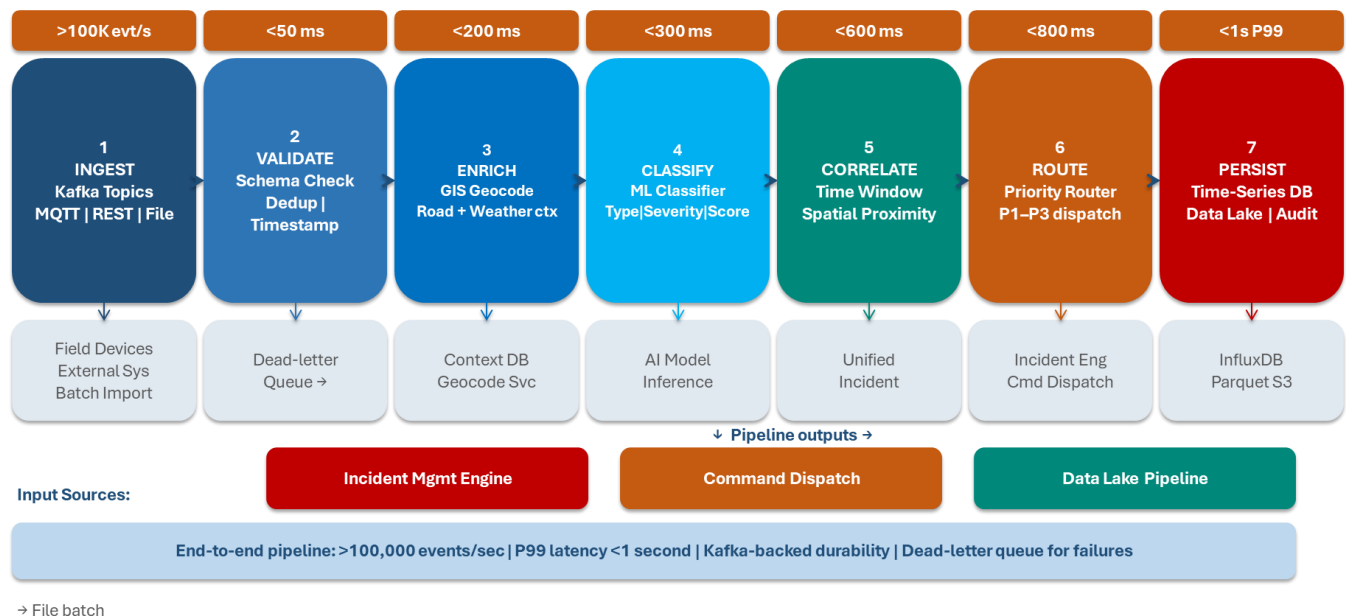


Figure 12: Event Processing Engine (EPE) — Data Flow Pipeline

#### 7.1.1.1. EPE Processing Pipeline

1. **Data Ingestion:** Raw events received via MQTT v5.0 (field devices), REST/Webhooks (external systems), and structured JSON feeds from vendor API (VIDES events, ANPR records, VMS status). Published to Kafka topics by source type.
2. **Data Validation:** Schema validation against the canonical data schema (CDS), duplicate detection using UUIDs and temporal deduplication, timestamp normalisation to UTC. Malformed or duplicate events quarantined to a dead-letter queue with alert generation.
3. **Data Enrichment:** Events enriched with contextual data — device GPS location (from GIS), road segment attributes, current weather readings (from 3<sup>rd</sup> Party System integration), and source attribution tag ('ATMS-native' or 'vendor-feed').
4. **Event Classification:** ML classifier assigns event type, severity, and confidence score. Events sourced from vendor feeds carry the vendor's original classification, which is preserved alongside the ATMS classification for audit transparency.
5. **Event Correlation:** The correlated event engine identifies related events within a configurable time window and spatial proximity (default: 500m radius, 5-minute window), grouping them into unified incident candidates for deduplication.
6. **Event Routing:** Classified and enriched events routed to Incident Processing Engine, Data Processing Pipeline, Alarm Engine, or Command Dispatch Engine as appropriate.
7. **Event Persistence:** All events persisted to the time-series database and national data lake for analytics and audit purposes.

**7.1.1.2. EPE Performance Requirements**

<b>Throughput</b>	≥ 100,000 events per second at NCCC tier; auto-scaling to 10× for peak events
<b>Processing Latency</b>	< 1 second end-to-end (receipt to routing)
<b>Reliability</b>	At-least-once delivery for all events; exactly-once for incident and enforcement events
<b>Horizontal Scalability</b>	Kubernetes HPA-driven; no manual intervention required
<b>Dead-Letter Management</b>	Failed events retained 7 days; automated retry with exponential back-off; DLQ alerting within 60 seconds

**7.1.2. Incident Processing Engine**

The IPE manages the complete lifecycle of all ATMS incidents from initial detection through resolution and post-incident review. It integrates with the GIS platform, SOP engine, notification engine, SLA monitoring engine, and external responder systems (iCAD, ERRS 112) to ensure coordinated, time-bounded incident response across all three tiers.

**7.1.2.1. Incident Lifecycle States**

State	Description	Entry / Exit Condition
DETECTED	Incident detected by any source — VIDES feed, ECB call, Rajmarg, manual etc.	Entry: Event from any source. Exit: Operator acknowledgement
ACKNOWLEDGED	Operator has reviewed and confirmed the incident	Entry: Operator ACK within SLA. Exit: Resources dispatched
DISPATCHED	Response resources assigned and notified via iCAD	Entry: iCAD dispatch confirmed. Exit: First resource at scene
IN PROGRESS	Response resources at scene managing the incident	Entry: Scene attendance confirmed. Exit: Road cleared
CLEARED	Carriageway cleared; traffic flow restored	Entry: Operator clearance confirmation. Exit: PIR complete
CLOSED	Post-Incident Review complete; record finalised	Entry: PIR accepted. Terminal state — immutable after 24 hrs

State	Description	Entry / Exit Condition
ESCALATED	SLA threshold breached; escalated to next command tier	Entry: SLA breach timer. Exit: Higher authority assumes control

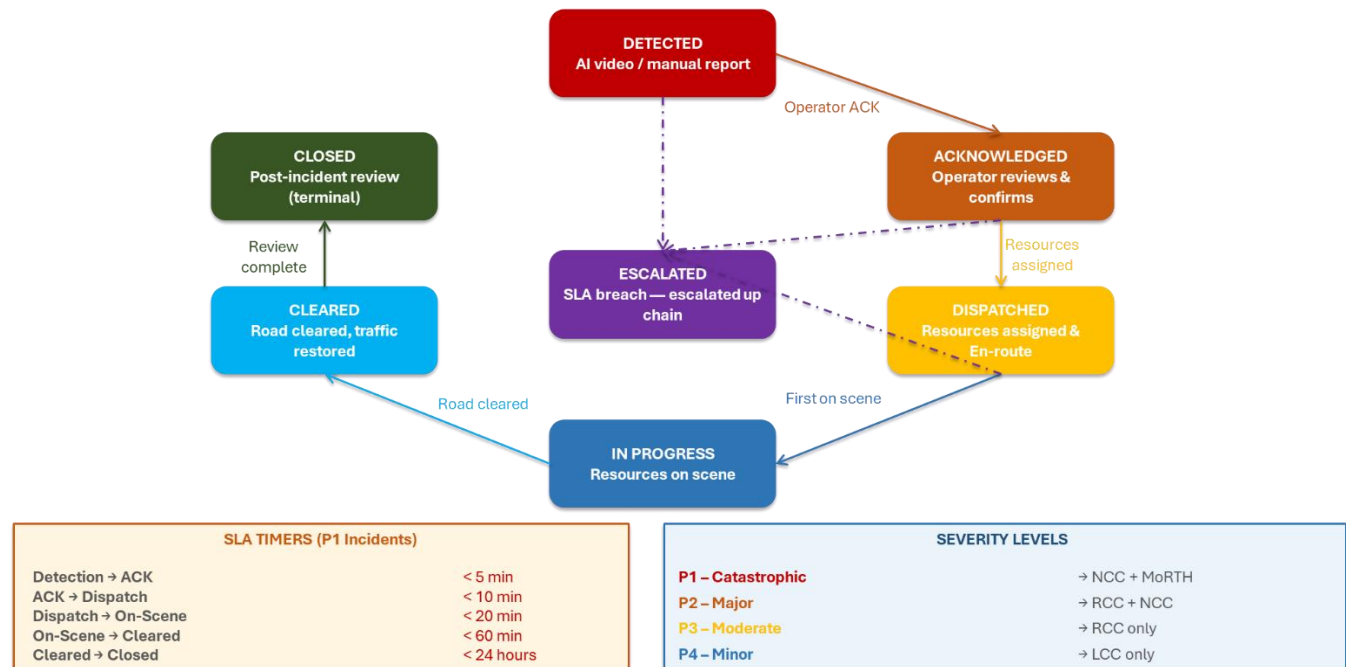


Figure 13: Incident Lifecycle — State Machine Diagram

### 7.1.3. Device Communication Engine

The Device Communication Engine (DCE) provides secure, reliable, bi-directional communication between the ATMS platform and all connected field devices. The DCE supports multiple communication protocols to accommodate the diversity of field devices deployed across the national highway network.

#### 7.1.3.1. Supported Protocols

1. MQTT v5.0 (Mandatory Primary): All ATMS-managed field device telemetry, events, and command dispatch. TLS 1.3 over port 8883. QoS Level 1 minimum. MQTT 3.1.1 for legacy devices only.
2. ONVIF Profile S/T: IP camera management (stream tokens, PTZ advisory, event notification). Note: PTZ commands are advisory requests forwarded to the vendor TMCS platform; the ATMS Platform does not directly manage camera hardware.
3. NTCIP 1203/TCP/IP: VMS advisory message requests forwarded to vendor VMS/VASD/Radar platform. ATMS receives VMS status via NTCIP/TCP/IP status polling from hardware.
4. Modbus TCP / DNP3: Legacy SCADA-type devices (certain weather station types, legacy signal controllers) if available.
5. SIP / VoIP: Integrated Audio Communication module — ECB/1033 call management.



- 
6. REST / HTTP (HTTPS): External API calls — all government system integrations (VAHAN, SARATHI, FASTag, iCAD, Rajmarg, IMD etc.) and Existing Field Platform Vendor API.
  7. SNMP v2c / v3: Network infrastructure monitoring (routers, switches, UPS).

#### **7.1.3.2. MQTT Topic Structure and Message Standard**

All hardware devices shall publish telemetry and events using a standardised MQTT topic hierarchy and JSON message envelope as defined in the ATMS Protocol Specification. This enables hardware vendor independence — any certified vendor's equipment integrates seamlessly with the software platform without custom adapters.

##### **7.1.3.2.1. MQTT Topic Hierarchy**

Mandatory topic format: `atms/{state_code}/{district_code}/{highway_id}/{gantry_id}/{data_type}`

- `atms/MH/PUNE/NH48/GNT001/speed` — Speed sensor telemetry
- `atms/MH/PUNE/NH48/GNT001/anpr` — ANPR camera data
- `atms/MH/PUNE/NH48/GNT001/event/violation` — Speed violation events
- `atms/MH/PUNE/NH48/GNT001/event/accident` — Accident detection events
- `atms/MH/PUNE/NH48/GNT001/status` — Device health (every 60 seconds)

##### **7.1.3.2.2. Standard Message Envelope**

All messages shall use this JSON structure: `{ "message_id": "UUID v4", "timestamp": "ISO 8601 UTC with ms precision", "source": { state, district, highway, gantry_id, device_id }, "payload": { /* data-type specific content */ } }`.

##### **7.1.3.2.3. Device Status Heartbeat**

All edge controllers shall publish device status every 60 seconds on the `/status` topic. Payload SHALL include: operational status (online/degraded/offline), CPU usage %, memory usage %, network latency ms, and per-sensor status array. Absence for more than 120 seconds SHALL trigger automatic device fault alert.

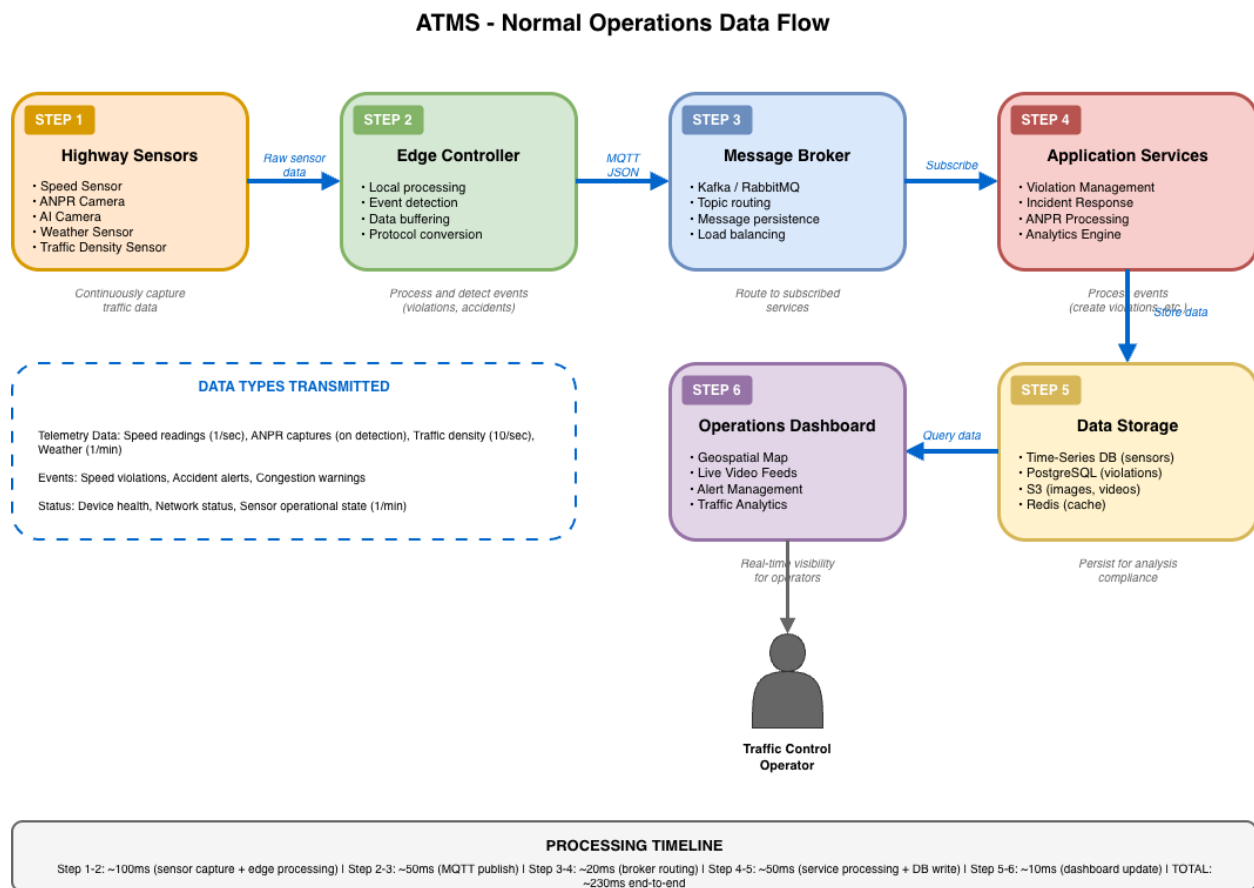


Figure 14: ATMS Normal Operations Data Flow

The specific technology stacks mentioned in the diagram are indicative. SDA is expected to propose their own stack with specific preference for opensource technologies and tools, with no proprietary lock-ins.

#### 7.1.4. Command Dispatch Engine

The CDE translates operational decisions — from operators, automated rules, or SOP workflows — into actionable requests and dispatches them to target systems. The CDE maintains a priority queue ensuring safety-critical commands (VMS speed limit advisories, NERS 112 notifications) are dispatched ahead of routine commands. All commands are logged with timestamp, originating user/system, command content, target system, and execution result.

1. VMS advisory message requests → forwarded to Existing Field Platform Vendor's VASD/VMS API
2. Camera PTZ advisory requests → forwarded to Existing Field Platform Vendor's TMCS API
3. iCAD dispatch commands → directly to 1033 iCAD system API
4. NERS 112 emergency notifications → directly to NERS 112 API
5. Rajmarg Yatra advisories → directly to Rajmarg API
6. ECB/1033 audio commands → to integrated audio communication engine

### **7.1.5. Real-Time Stream Processing**

Built on Apache Kafka and Apache Flink / Spark Structured Streaming or similar, the stream processing layer handles continuous ingestion and transformation from all sources. Stream processing jobs are containerised microservices deployed within Kubernetes, enabling independent scaling. A declarative pipeline DSL allows pipeline updates without system downtime via rolling deployment.

Key stream types processed: ATMS device health telemetry, AWS sensor data, ECB/1033 event streams, vendor VIDES incident events, vendor ANPR/TTMS data feeds, vendor VMS status updates, vendor e-challan lifecycle updates, and external government API response events.

## **7.2. UNIFIED NATIONAL GIS PLATFORM**

The Unified National GIS Platform provides the geographic intelligence layer for the National ATMS. It delivers a real-time, interactive map-based operational view of the entire national highway network, including live traffic conditions, incident locations, device health, enforcement activities, and weather conditions. FRS Modules: HTM (Highway Traffic Monitoring & GIS Dashboard), GIS (Extended GIS Platform). The GIS platform provides the geographic intelligence layer and Common Operating Picture (COP) for all three command tiers. It is built on opensource GIS solutions and shall be custom-built for project specific demands.

The GIS platform is accessible at all command levels (NCCC, RCCC, LCCC) with role-based views appropriate to each level and shall be integrated with national level GIS platforms for data analysis and reporting.

### **7.2.1. GIS Engine**

The GIS engine is built on an open-source spatial database . The system supports both raster and vector tile formats, with vector tiles used for dynamic, data-driven visualisation of traffic conditions, incident locations, and device status.

The GIS engine ingests and maintains the following base data layers: national highway network centerlines and attributes; toll plaza locations and attributes; kilometre post (KP) reference system; administrative boundaries (state, district); emergency services locations (hospitals, police stations, fire stations); and weather grid data.

The GIS engine maintains all national highway base data layers: highway network centerlines and attributes, toll plaza locations, KP reference system, administrative boundaries, and POI database (hospitals, police stations, fire stations, petrol pumps, rest areas, airports). Vector tiles are used for dynamic, data-driven visualisation of live traffic conditions, incidents, and device health. Both OpenStreetMap and commercial tile providers (Google Maps, Bing, ESRI or similar) are supported, with an offline cached base map for all LCCC corridors updated weekly.

### **7.2.2. Real-Time Traffic Visualization**

Traffic conditions are visualised using a colour-coded speed band overlay on the highway network. The speed band is calculated from radar sensor data and ANPR journey time data, updated every 60 seconds under normal conditions and every 15 seconds during incidents. The following speed bands are used: Green (>80% of speed limit), Amber (40-80%), Red (<40%), Black (0 – road closed), and Purple (incident location).

Traffic volume heatmaps, time-series speed charts, and turning movement counts are available for each sensor location through an interactive pop-up panel. Operators can replay historical traffic conditions for any time period using the time-slider interface.

Traffic speed, volume, vehicle classification, and journey time data all sourced from existing Field Platform Vendor's ATCC/VIDES/TTMS platform via Data Exchange Specification API. Road condition shall also be marked on the map in different category based on the data received from various ATMS sensors (Cameras, Radar, etc.).

### **7.2.3. Incident Visualization**

The GIS map supports the following independently toggleable layers, all updated in real time:

1. Incident Layer: Active incidents with severity-coded icons (severity from ATMS IPE). Clicking opens full incident record with SOP progress, nearest camera stream token, weather, and SLA countdown.
2. ITS Device Layer: All registered CCTV/TMCS, ANPR/VIDS, VMS,VASD, RADAR, ATCC, RLVD, SLVD, WIM, ECB, and AWS devices with health-status icons (health sourced from ATMS NMS for ATMS-managed devices; from vendor NMS telemetry feed for vendor-managed devices).
3. Traffic Speed Layer: Colour-coded speed bands from vendor ATCC/VIDS feed.
4. Weather Layer: Real-time AWS readings with threshold-breach colour coding.
5. Emergency Vehicle Tracking: Live GPS of RPVs, ambulances, cranes from AIS-140/iCAD.
6. Crowd-Sourced Event Layer: Incidents from 1033 iCAD, Rajmarg Yatra, NHAI App — geo-tagged and distinguished from sensor/AI events by icon style.
7. Enforcement Activity Layer: Active enforcement events from vendor e-Challan feed.
8. Camera FOV Overlay: Field-of-view cones for coverage gap analysis.
9. Heat Maps: Incident frequency, violation frequency, congestion — over user-defined time ranges.

### **7.2.4. Incident Detection Workflow**

1. Vendor VIDES or ANPR/VSDS structured event received by EPE API ingestor.
2. EPE geo-codes event to nearest KP reference using GIS spatial index.
3. IPE creates incident record; GIS incident layer updated within 5 seconds.
4. GIS map auto-pans to incident KP; operator receives visual + audio alert.
5. Operator reviews evidence (stream token from vendor TMCS, ANPR data) via GIS pop-up, confirms or dismisses.
6. On confirmation, GIS shows resource dispatch map (iCAD vehicle positions, ETAs, nearest hospital from POI database).
7. GIS updates continuously as incident progresses through lifecycle states

---

### 7.3. NATIONAL API GATEWAY PLATFORM

The National API Gateway is the single authorised entry point for all external system integrations and third-party access to National ATMS data. It provides centralized authentication, authorisation, rate limiting, API versioning, request routing, and audit logging for all API interactions.

#### 7.3.1. API Gateway Architecture

Deployed as a horizontally scaled cluster (Kong, Netflix Zuul, or equivalent gateway) behind a global load balancer. Supports REST (JSON/XML) and WebSocket interfaces. All traffic logged to centralised audit log. IP whitelisting available as additional control for high-security government integrations. mTLS used for police, courts, and DMC/SDMA integrations.

#### 7.3.2. Authentication and Authorization Framework

- OAuth 2.0 Client Credentials Flow: All third-party government system integrations (VAHAN, SARATHI, FASTag/NETC, State ICCCs, DMC/SDMA, Rajmarg, NHAI App).
- JWT (JSON Web Tokens): Stateless API authentication for platform operators and internal service-to-service calls.
- API Keys: Machine-to-machine integrations with government databases.
- mTLS (Mutual TLS): Police PCR feed, eCourts/NJDG, and DMC/SDMA — high-security government integrations requiring certificate-based mutual authentication.
- Access Token Expiry: Maximum 1 hour (3,600 seconds); automatic refresh via token rotation.
- Rate Limiting: Configurable per client; default 1,000 requests/hour; HTTP 429 on breach.

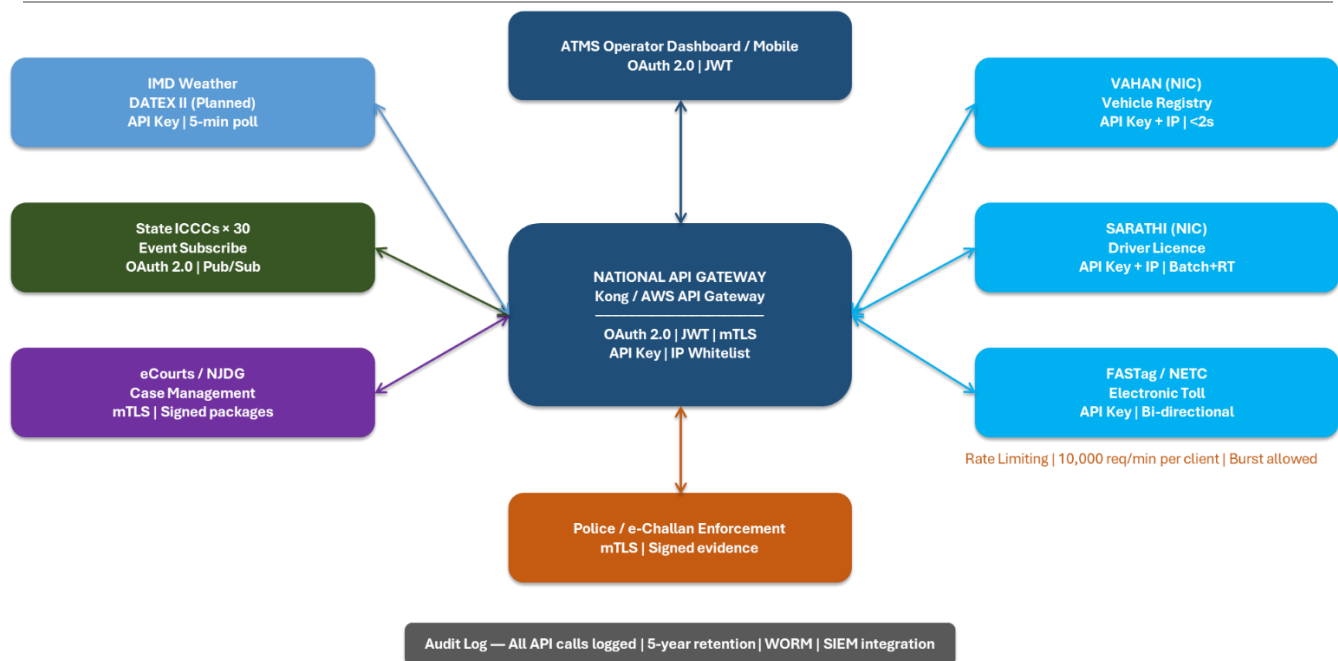


Figure 15: National API Gateway Integration Architecture

### 7.3.2.1. Mandatory Government System Integrations (Not only limited to)

Integration	Purpose	Latency Target	Availability Target	Protocol / Auth
VAHAN (NIC)	Vehicle registry — owner, registration, insurance, fitness, PUC	<2s	99.5%	REST/JSON + OAuth 2.0
SARATHI (NIC)	Driving licence, penalty points	<2s	99.0%	REST/JSON + OAuth 2.0
FASTag/NETC (NPCI)	Toll transaction confirm + evasion alerts	<5s	99.5%	REST/JSON + API Key
NIC Enforcement Portal	e-Challan status updates from vendor enforcement	<5s	98.0%	REST/XML + PKI cert
eCourts/NJDG	Defaulted challan transmission	<120s	97.0%	SFTP + Digital Signature
CCTNS (Police)	Vehicle verification, blacklist check, incident linking	<30s	98.0%	REST + mTLS

Integration	Purpose	Latency Target	Availability Target	Protocol / Auth
1033 iCAD	Bidirectional incident dispatch and tracking	<10s	99.0%	REST/JSON + OAuth 2.0
Rajmarg Yatra	Crowd reports in; traffic advisories out	<30s	98.0%	REST/JSON + API Key
NHAI Mobile App	Live traffic, incidents, VMS messages, 1033 CTC	<15s	99.0%	REST/JSON + OAuth 2.0
NERS 112	Major/Catastrophic incident notification	<2min	99.5%	REST/JSON + mTLS
IMD API	National weather forecasts	<5min	95.0%	REST/JSON + API Key
AIS-140	Patrol vehicle GPS tracking	<30s	98.0%	REST/JSON + OAuth 2.0
DigiLocker	Enforcement evidence sharing	<60s	97.0%	REST/JSON + OAuth 2.0
PM Gati Shakti GIS	Traffic, incident, asset data sharing	<5min	95.0%	REST/GeoJSON
State ICCCs	Bidirectional event sharing	<30s	99.0%	DATEX II v3.2 / REST
DMC/SDMA	Emergency event push + corridor status	<2min	99.0%	REST + NDMA schema + mTLS
Police PCR (video feed)	CCTV stream token sharing over dedicated circuit	<5s	99.5%	RTSP tokens + MPLS/OFC
IHMCL DataLake/ERP	End-of-day ATMS operational data push	Daily	99.0%	REST/JSON + OAuth 2.0
Existing Field Platform Vendor	VIDES events, ANPR data, VMS status, e-Challan, NMS telemetry	<5–60s	99.5%	REST/MQTT + OAuth 2.0 (DES)

### 7.3.2.1.1. VAHAN Integration (Vehicle Registry)



The VAHAN integration provides real-time and batch query capabilities for vehicle registration details. The ATMS uses VAHAN primarily for enforcement workflows (owner identification for challans) and traffic analysis (vehicle type classification). The integration uses the VAHAN API exposed through NIC, authenticated using API key and IP whitelisting.

- Vehicle Registration Certificate (RC) query by registration number.
- Insurance validity check by registration number.
- Fitness certificate validity check.
- Emission (PUC) certificate validity check.
- Batch query mode for overnight reconciliation of enforcement records.

#### **7.3.2.1.2. SARATHI Integration (Driver Licence)**

SARATHI integration enables the ATMS to link driver licence data to enforcement records, enabling penalty points tracking and repeat offender identification. The integration uses the SARATHI API exposed through NIC, authenticated using API key and IP whitelisting.

- Driver Licence (DL) query by DL number.
- Penalty points query and update by DL number.
- Disqualified / suspended licence check.

#### **7.3.2.1.3. FASTag / NETC Integration**

The FASTag integration is one of the most critical integrations in the National ATMS ecosystem. It enables the ATMS to link every FASTag transaction at every toll plaza with the corresponding ANPR capture, enabling real-time journey time calculation, vehicle tracking for incident investigation, and enforcement of vehicles that evade toll. The integration is bidirectional: the ATMS receives transaction data from the NETC switchboard in real-time and sends enforcement flags back to NETC for vehicles that have outstanding challans.

#### **7.3.2.1.4. Police Enforcement Integration**

The police integration enables seamless handover of enforcement evidence and challan records from the ATMS to state and national highway police enforcement systems. The integration supports the NIC e-challan framework (VAHAN-linked) and direct integration with State Police IT systems via REST API. All challan records are cryptographically signed to ensure admissibility as legal evidence. The system shall also be integrated with *crime and Criminal Tracking Network & Systems (CCTNS)*.

#### **7.3.2.1.5. Court System Integration**

Integration with the National Judicial Data Grid (NJDG) and eCourts system enables automatic filing of enforcement cases that are not settled within the prescribed period. The integration transmits digitally signed evidence packages (images, video clips, ANPR records, VAHAN data) to the court system and receives updates on case status, adjournment dates, and verdicts.

#### **7.3.2.1.6. State ICCC Integration**

State Integrated Command and Control Centres are integrated with the National ATMS through the API Gateway using a publish-subscribe model wherever available. The ATMS publishes real-time traffic events, incidents, and weather data to state ICCC subscribers within each state's geographic boundary. State ICCCs may also push events to the ATMS (such as incidents reported through state police channels) using the ATMS Inbound Event API.

### 7.3.2.1.7. Per-Integration Non-Functional Requirements

The following NFRs specify quantitative performance and availability targets for each mandatory government system integration.

NFR ID	Integration	Latency P95	Availability	Auth Method	Critical Notes
<b>NFR-INT-VHN</b>	VAHAN	<2s	99.5%	OAuth 2.0 / NIC key	Mandatory for ANPR challan; outage triggers queuing mode with 72h retry
<b>NFR-INT-SAR</b>	SARATHI	<3s	99.0%	OAuth 2.0 / NIC key	Driver licence validation; degraded mode: skip if unavailable; event logged
<b>NFR-INT-FAS</b>	FASTag/NETC	<5s	99.9%	IHMCL signed JWT	Critical for toll revenue; FASTag status required per vehicle passage; high availability mandatory
<b>NFR-INT-POL</b>	Police e-Challan	<60s	98.0%	SFTP/REST + PKI cert	Challan evidence package upload; 5 retries on failure; undelivered challans flagged in SLA dashboard
<b>NFR-INT-CRT</b>	eCourts/NJDG	<120s	97.0%	SFTP + Digital Sig.	Unpaid challans escalated after 30 days; batch processing OK; audit trail mandatory
<b>NFR-INT-SIC</b>	State ICCCs	<30s	99.0%	DATEX II / REST+TLS	Bidirectional incident sharing; DATEX II v3.2; state ICCC availability only affects shared incidents

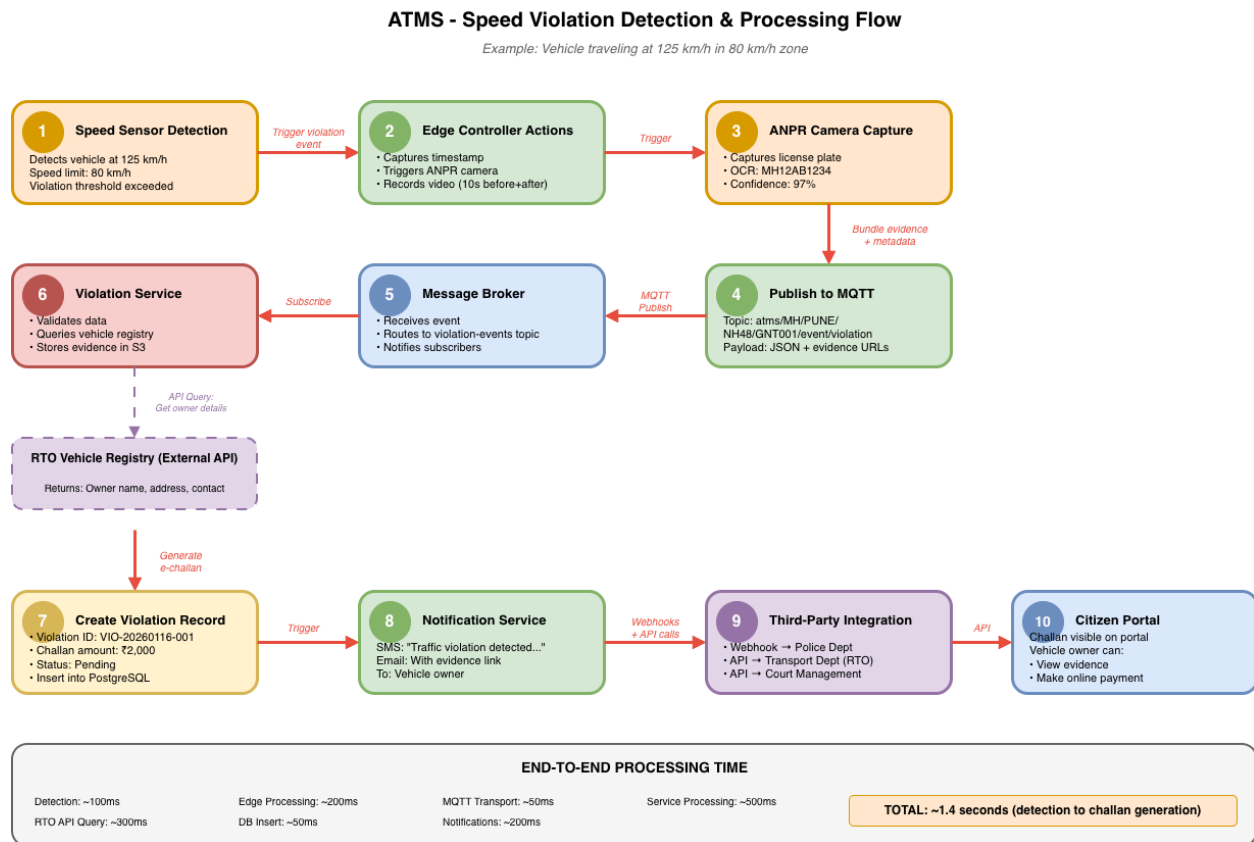


Figure 16: ATMS Violation Detection and Processing Flow (Step 1 to 4 would happen at Vendor provided VIDES system)

The specific technology stacks mentioned in the diagram are indicative. SDA is expected to propose their own stack with specific preference for opensource technologies and tools, with no proprietary lock-ins.

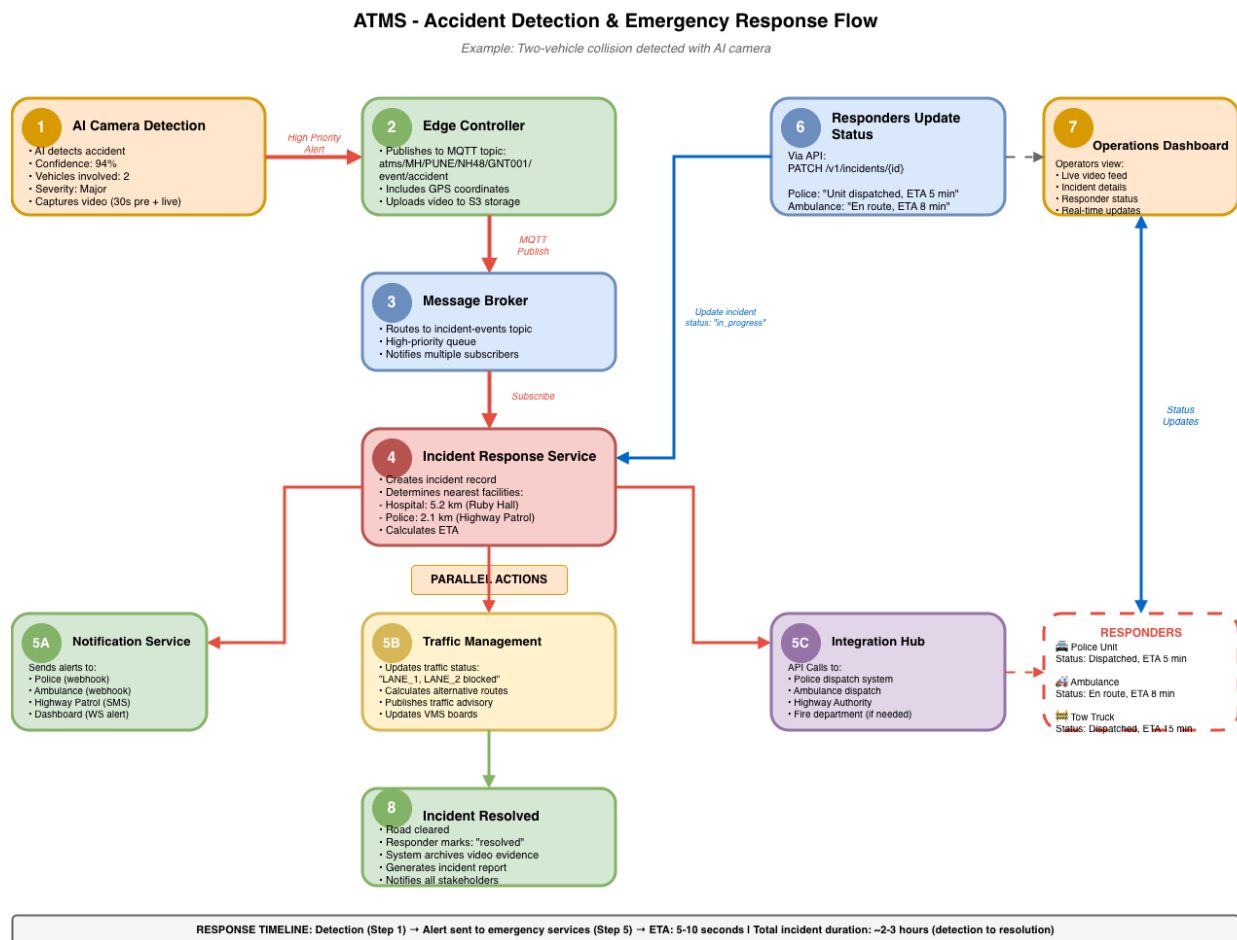


Figure 17: ATMS Incident Response Flow

The specific technology stacks mentioned in the diagram are indicative. SDA is expected to propose their own stack with specific preference for opensource technologies and tools, with no proprietary lock-ins.

## 7.4. Vendor Data Interface Layer

ANPR plate recognition, speed enforcement computation, journey time computation (TTMS), video analytics/VIDES incident detection, violation evidence capture, e-Challan generation, and VMS content authoring are all Existing Field Platform Vendor functions. The ATMS Platform receives their structured outputs via this interface layer.

### 7.4.1. Vendor Data Interface Layer — Architecture

The Vendor Data Interface Layer (VDIL) is a dedicated ingestion sub-system within the ATMS API Gateway that manages all inbound data streams from the Existing Field Platform Vendor. It provides schema validation, data normalisation, version management, and health monitoring for all vendor data feeds.

### 7.4.2. Vendor Interface Catalogue

Vendor System	Data Delivered to ATMS	Frequency / Trigger	Format	ATMS Action
VIDES / TMCS	Structured incident detection events: incident type, camera ID, KP, severity, confidence score, thumbnail URL, bounding box metadata	≤5 sec post-detection	JSON/REST	ATMS creates incident record; sends ACK back to vendor
ANPR / VSDS / TTMS/VASD/RADAR	Vehicle passage records: plate, class, camera ID, KP, direction, speed; journey times per ANPR pair; speed violation flags	≤60s aggregate; ≤10s per violation event	JSON/MQTT	ATMS displays on GIS; feeds analytics; escalates to watch-list alerts
VMS	VMS device status, current displayed message, last command ACK timestamp, device health state	≤60s interval	JSON/REST	ATMS displays on GIS; computes VMS uptime SLA
enforcement / e-Challan	Violation records and challan lifecycle status: generated, notified, paid, disputed, defaulted, settled	≤5 min per state change	JSON/REST	ATMS feeds reporting, analytics, NIC portal relay, regulatory dashboards
EMS/ NMS	Device health telemetry for VIDES, ANPR, VMS, speed radar units, Network devices etc.: online/offline/degraded, fault events, restoration timestamps	≤5 min interval	JSON/SNMP	ATMS computes vendor device SLA; feeds asset registry
ATCC / Traffic Counter	Vehicle count, classification, occupancy, speed, headway per lane per direction	≤60s interval	JSON/REST	ATMS displays traffic speed layer on GIS; feeds analytics

#### 7.4.3. VDIL Technical Standards

- All interfaces governed by the Data Exchange Specification (DES) agreed between IHMCL, the ATMS SDA, and the Existing Field Platform Vendor before go-live.

- Standard data format: JSON or XML over HTTPS REST; MQTT for high-frequency telemetry.
- Authentication: OAuth 2.0 / API key per interface; all credentials managed in the ATMS secrets vault.
- Schema versioning: All vendor feed schemas version-tagged in the System Integration Register; schema mismatch alerts generated within 60 seconds.
- Feed health monitoring: Last successful receive timestamp, message volume per hour, error rate, and schema validation failure rate tracked per feed. Alert if any feed silent for >2× expected interval.
- Vendor data attribution: All data received from vendor feeds tagged with 'vendor\_source: true' throughout the data pipeline for audit and explainability transparency.

## 7.5. NATIONAL DATA LAKE ARCHITECTURE

The National Data Lake provides the long-term storage and analytics infrastructure for all data generated by the National ATMS. It is designed to scale to 10+ petabytes of stored data, accommodate data from 100,000+ devices across 50,000+ km of national highways, and support both real-time analytical queries and complex historical analysis.

### 7.5.1. Data Architecture Layers

<b>Raw Zone (Bronze)</b>	Immutable landing zone. All ingested data stored in original format in Apache Parquet on object storage, partitioned by date, source type, and geographic zone. Serves as system of record for replay and reprocessing.
<b>Processed Zone (Silver)</b>	Cleaned, validated, enriched data. Transformations: deduplication, schema normalisation, geospatial KP enrichment, weather enrichment, vendor_source attribution tagging, quality scoring. Apache Parquet / Delta Lake format.
<b>Analytics Zone (Gold)</b>	Aggregated, pre-computed datasets for analytical query performance: traffic flow summaries (hourly/daily/monthly), incident statistics, enforcement statistics (from vendor feed), device availability reports, SLA metrics. Data source for all dashboards, reports, and APIs.

#### 7.5.1.1. Raw Data Zone (Bronze)

The Raw Data Zone stores all ingested data in its original format, unmodified, with no transformations applied. This zone serves as the system of record for all data received, enabling re-processing in case of downstream processing errors. Data is stored in Apache Parquet format on object storage, partitioned by date, data source type, and geographic zone.

#### 7.5.1.2. Processed Data Zone (Silver)

The Processed Data Zone contains cleaned, validated, and enriched data derived from the raw zone. Transformations include: deduplication, schema normalisation, geospatial enrichment (KP reference, road

segment), VAHAN enrichment (vehicle type, owner category), and quality scoring. Data in this zone is stored in Apache Parquet or Delta Lake format.

### 7.5.1.3. Analytics Data Zone (Gold)

The Analytics Data Zone contains aggregated, pre-computed datasets optimised for analytical query performance. This includes: traffic flow summaries (hourly, daily, monthly), incident statistics, enforcement statistics, device availability reports, and SLA performance metrics. This zone serves as the data source for all dashboards, reports, and data sharing APIs.

### 7.5.2. Data Categories, Volume and Retention

Environment	On Prem Server Infra	Cloud DR Required	Data Retention on Premise (Days)	Locations	Storage and Retention Policy
LCCC	Yes	No	7	667	LCCC locations shall push data to their respective RCCs over secure internet connectivity.
RCCC	Yes	No	30 Days (Hot Storage)+180 Days (Archival)	20	<ol style="list-style-type: none"> <li>1. RCCC locations (On Premise Server) shall push the data to NCCC central Servers &amp; Storage (On Premise)</li> <li>2. Data includes: All incident data with images, video clips (incidents and speed violation etc.) as received from LCCC, including e-challan incidents.</li> <li>3. Each RCCC location shall maintain on-premises SAN storage capacity of 250 TB and NAS storage of 1 PB to retain data for a period of 30 and 180 days respectively.</li> </ol>
NCCC	Yes	Yes	10 Years + Critical Events as per requirements	1	<ol style="list-style-type: none"> <li>1. Only Meta Data shall be stored at NCCC level (i.e. excluding Images, Audio, Video clips).</li> <li>2. 5 PB SAN storage shall be required for retention of Meta data at NCCC on premises.</li> <li>3. Deployment of Common NHAI ATMS SW at NCCC level- control</li> </ol>



					DC (On Premises & DR on Cloud). No data shall be stored on cloud only application to be deployed on cloud DR.
--	--	--	--	--	--

The data to be stored from following sensors:

- 1 TMCS/PTZ (Video)
- 2 VIDES (Image/Video)
- 3 ANPR (Image/Video)
- 4 VASD (Logs)
- 5 Radar (Logs)
- 6 VMS (Logs)
- 7 Met System (Logs)
- 8 ECB (Audio)
- 9 Security/NMS (Logs)

#### 7.6. AI and Predictive Analytics Engine

The analytics sub-platform provides predictive models running on the ATMS SW. All AI predictions carry a confidence score and are labelled 'AI Estimate' — never presented as operational facts.

- Congestion Prediction: 1-hour and 4-hour ahead forecasts per corridor segment; ≥80% accuracy; updated every 15 minutes.
- Incident Risk Prediction: Road segments and time periods with elevated probability based on historical incidents, weather, traffic volume (from vendor feed), and temporal patterns.
- Predictive Device Maintenance: Devices with elevated failure probability within 30 days based on age, fault history, MTBF statistics, and environmental data.
- Weather-Incident Correlation: Historical weather event + incident record correlation per corridor, updated quarterly; feeds incident risk model.
- Model Performance Monitoring: Monthly automated evaluation; accuracy metrics published to System Admin dashboard; bi-annual retraining cycle.

#### 7.7. SLA, ASSET, INCIDENT, AND CONTRACT MONITORING ENGINE

The SLA and Asset Management platform provides NHAI and IHMCL with comprehensive visibility into the performance of all ATMS technology service providers (TSPs), the health and lifecycle status of all deployed field assets, and the compliance of all ATMS projects with contractual obligations. Dashboards shall be available at all tiers (LCCC, RCCC, and NCCC) for real-time monitoring of system performance and operational status. The NCCC shall have visibility across all RCCCs and LCCCs. Each RCCC shall have visibility over its respective LCCCs within its jurisdiction. The LCCC shall have access limited to monitoring its own systems and status only.

#### Asset Lifecycle Management

Every field asset deployed under the National ATMS programme is registered in the Asset Registry, which is the authoritative master record for all devices. The Asset Registry maintains the complete lifecycle record of each device from procurement through commissioning, operation, maintenance, and decommissioning.

#### 7.7.1. Asset Registry Data Model

- Asset Identification: Asset ID, Serial Number, Make, Model, Firmware Version.
- Location: KP Reference, GPS Coordinates, Highway Name, Project Name.
- Status: Operational, Faulty, Under Maintenance, Decommissioned.
- Lifecycle: Procurement Date, Commissioning Date, Last Maintenance Date, Next Planned Maintenance Date, Warranty Expiry Date.
- Ownership: Contractor, Contract Number, TSP Responsibility Zone.
- Connectivity: Communication Protocol, IP Address, Port, Gateway Node, Last Seen Online.

<b>Asset Identification</b>	Asset ID (globally unique), Serial Number, Make, Model, Hardware Version, Firmware Version
<b>Location</b>	KP Reference, GPS Coordinates (WGS84), Highway Name, Project Name, Corridor ID
<b>Status</b>	Operational   Faulty   Under Maintenance   Decommissioned   Pending Commissioning
<b>Lifecycle</b>	Procurement Date, Commissioning Date, Last Maintenance Date, Next Planned Maintenance Date, Warranty Expiry Date, Expected Service Life (years)
<b>Ownership</b>	Contractor, Contract Number, TSP Responsibility Zone, ATMS Project
<b>Connectivity</b>	Communication Protocol, IP Address, Port, Gateway Node, Last Seen Online, Data Source ('ATMS-native' or 'vendor-reported')

#### 7.7.2. SLA Compliance Engine

The SLA Compliance Engine monitors real-time device and system performance against the contracted SLAs for each ATMS project. SLA metrics are computed automatically from device telemetry data, incident records, and maintenance logs, without manual data entry by TSPs.

SLA Metric	Target Threshold	Computation Method & Data Source
ATMS Platform Availability (NCCC)	≥99.9% per month	Automated uptime computation from APM platform — ATMS-native

SLA Metric	Target Threshold	Computation Method & Data Source
ATMS Platform Availability (RCCC)	≥99.5% per month	Automated uptime computation — ATMS-native
LCCC Online Rate	≥95% of commissioned LCCCs	MQTT heartbeat monitoring — ATMS-native
CCTV/TMCS Camera Availability (vendor-reported)	≥95% per month	Vendor NMS telemetry feed — attributed as 'vendor-reported' in SLA report
ANPR Read Accuracy (vendor-reported)	≥98% per month	Vendor ANPR platform feed — attributed as 'vendor-reported'
VMS Uptime (vendor-reported)	≥99% per month	Vendor VMS/VASD/RADAR status feed — attributed as 'vendor-reported'
P1 Incident Response Time	≤15 minutes	iCAD dispatch timestamp vs IPE detection timestamp
Data Ingestion Latency	≤5 seconds	Measured at EPE ingestor vs field device origination timestamp
Government API Uptime	≥99.0%	ATMS API Gateway health monitoring

## 7.8. CYBERSECURITY ARCHITECTURE

The National ATMS is classified as a Critical Information Infrastructure (CII) under the NCIIPC framework. Its cybersecurity architecture is therefore designed to the highest standards applicable to national critical infrastructure, implementing controls aligned with CERT-In guidelines, NCIIPC directives, ISO 27001:2022, and NIST Cybersecurity Framework.

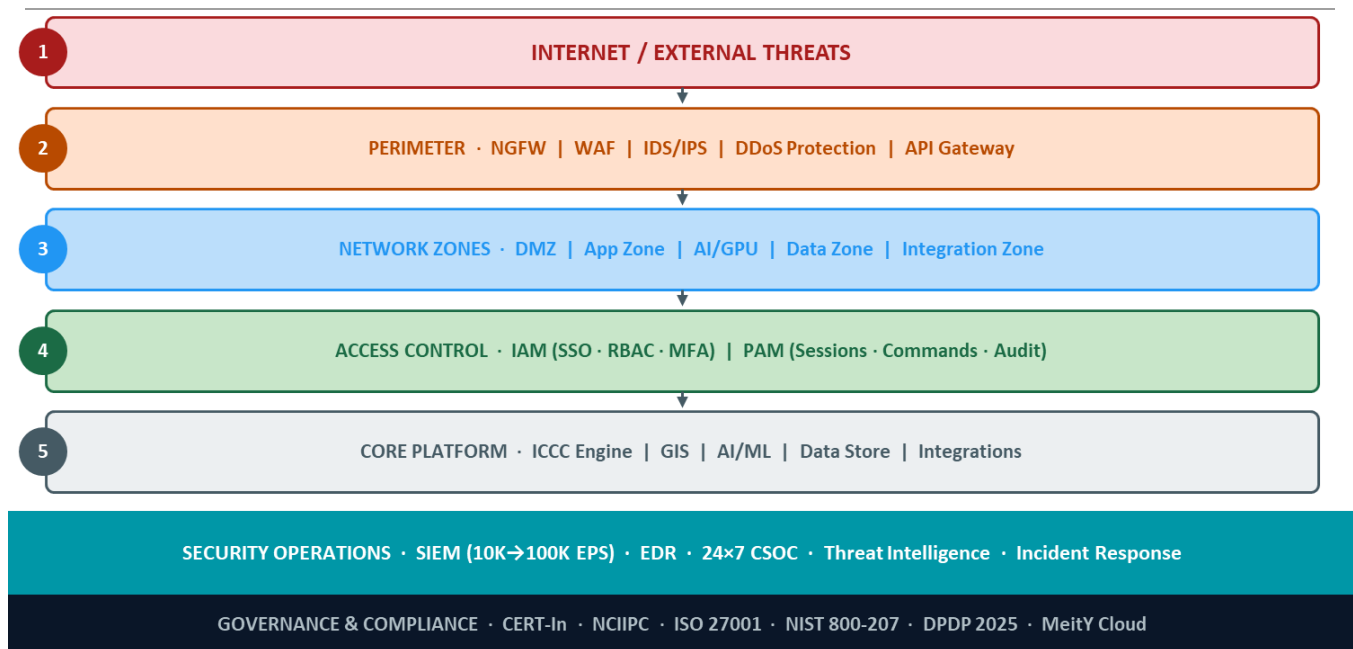


Figure 18: Cyber Security Framework

### 7.8.1. Zero Trust Architecture

No network location is implicitly trusted. Every access request — regardless of network origin — is validated against the IAM policy in real time. ZTA applies to all connections including LCCC-to-RCCC, inter-service microservice calls, and all API connections to Existing Field Platform Vendor systems.

1. Kubernetes Network Policies: Default-deny for all pod-to-pod communication; only explicitly permitted inter-service traffic allowed.
2. Service Mesh: Istio or Linkerd or similar for mTLS between all internal microservices; traffic encrypted even within the cluster.
3. Micro-segmentation: NCCC, RCCC, LCCC, API Gateway, Data Lake, SIEM, and Administration are isolated network zones.
4. Privileged Access Management (PAM): JIT (Just-in-Time) privileged access; no standing privileged accounts except break-glass. All privileged sessions recorded (keystrokes + screen).

#### 7.8.1.1. Zero Trust Principles Applied

- **Verify Explicitly:** Every access request is authenticated using multi-factor authentication. Devices are validated using certificate-based device identity.
- **Least Privilege Access:** Users and systems are granted the minimum level of access required to perform their function. Privileged access is time-limited and requires additional approval.
- **Assume Breach:** The system is designed assuming that any component may be compromised. Lateral movement is prevented through micro-segmentation. All traffic is monitored for anomalies.
- **Continuous Validation:** Access tokens are short-lived (maximum 1 hour). Re-authentication is required for sensitive operations. Behavioural analytics detect anomalous access patterns.

**7.8.1.2. Identity and Access Management (IAM)**

The ATMS IAM system manages the identity lifecycle for all human users, service accounts, and devices. It implements role-based access control (RBAC) with attribute-based access control (ABAC) extensions for fine-grained authorisation. The IAM system integrates with the NIC National Identity Framework (NIF) for human user authentication and with the ATMS PKI for device identity.

**7.8.1.3. IAM User Roles**

Role	Level	Permissions Summary
National Operations Director	NCCC	Full read/write on all NCCC data; approve national VMS campaigns; manage RCC operators
NCCC Senior Operator	NCCC	Read all data; manage national incidents; approve escalated RCC incidents
NCCC Operator	NCCC	Read NCCC dashboard; manage assigned incidents; read-only for device management
Regional Director	RCCC	Full read/write on regional data; approve regional VMS campaigns; manage LCCC operators
RCCC Operator	RCCC	Read regional data; manage regional incidents; dispatch resources
LCCC Senior Operator	LCCC	Read/write LCCC data; manage local incidents; manage local devices; approve local VMS
LCCC Operator	LCCC	Read LCCC data; manage assigned incidents; limited device control
Field Maintenance	LCCC/Field	Read device status; create/update maintenance tickets; cannot manage traffic or incidents
Police Liaison	RCCC/LCCC	Read incident data; access enforcement records; cannot modify ATMS configuration
System Administrator	NCCC	System configuration; user management; no access to operational incident/enforcement data

**7.8.2. Encryption Architecture**

1. Data at Rest: AES-256 for all databases, file stores, enforcement evidence, call recordings, and backup media. Keys managed by MEITY-approved KMS/HSM or NIC Key with automatic rotation every 12 months.
2. Data in Transit: TLS 1.3 minimum for all network communication. TLS 1.0/1.1 disabled. SRTP for audio streams.

3. Edge Device Certificates: X.509 certificates for MQTT TLS authentication; 12-month rotation via automated PKI; revocation within 60 seconds via OCSP/CRL.
4. Evidence Integrity: All enforcement evidence and call recordings digitally signed at capture; any modification invalidates signature and generates SIEM alert.

#### 7.8.2.1. Threat Monitoring and SIEM

The ATMS Security Information and Event Management (SIEM) platform collects security event logs from all ATMS components including application logs, infrastructure logs, network flow logs, and physical security logs. The SIEM applies correlation rules and machine learning models to detect threats in real-time. Alerts are triaged by the 24x7 Cybersecurity Operations Centre (CSOC) team.

CERT-In mandatory incident reporting timelines are embedded in the CSOC standard operating procedures: critical cyber incidents must be reported to CERT-In within 6 hours of detection as per the CERT-In Directions 2022. The SIEM system generates automated draft CERT-In incident reports to accelerate compliance.

### 7.9. TESTING AND PERFORMANCE ENGINEERING FRAMEWORK

The National ATMS Testing Framework defines the comprehensive approach to validating system quality, performance, resilience, and security across all deployment environments. The framework aligns with IEEE 29119 Software Testing Standards and incorporates specialised methodologies for ITS system testing.

#### 7.9.1. Load Testing Architecture

Load testing is performed using a distributed load generation framework capable of simulating the full load profile of the national ATMS: 100,000+ concurrent device connections, 10 million vehicle records per day, 1 million API calls per hour, and 50,000 concurrent dashboard users. Apache JMeter or Locust or similar are used as load generation tools, orchestrated through a Kubernetes-based test cluster.

#### 7.9.2. Performance Testing Targets

Performance Metric	Target (Normal Load)	Target (Peak Load)	Test Method
Dashboard Load Time	<2 seconds	<5 seconds	Selenium + JMeter
GIS Map Render Time	<3 seconds	<8 seconds	JMeter + WebDriver
API Response (P95)	<500ms	<1500ms	JMeter load test
Incident Detection Latency	<5 seconds	<5 seconds	Synthetic video injection
ANPR Inference Latency	<80ms per frame	<100ms per frame	Frame injection test
Database Query (P99)	<200ms	<500ms	pgBench + JMeter

### 7.9.3. Failover and DR Testing

Failover and disaster recovery testing is mandated quarterly for the NCCC Kubernetes pod-level failover validation. The full DC→DR failover simulation is mandated annually (Q4 of each O&M year) per SLA-19, validating both RTO <2 hours and RPO <4 hour. Tests are performed in a production-mirror test environment. Each test generates a failover test report witnessed by IHMCL and the IA's DR Test Manager

### 7.10. GOVERNANCE AND MONITORING PLATFORM

The Governance and Monitoring Platform provides stakeholders at all levels of the command hierarchy with the dashboards, reports, and analytics tools needed to exercise informed oversight of the National ATMS programme.

<b>National Dashboard (NCC)</b>	Real-time national incident rate, enforcement revenue (from vendor e-Challan feed), device availability heatmap, cross-regional comparison, programme KPI RAG status for MoRTH/IHMCL/NHAI leadership.
<b>Regional Dashboard (RCCC)</b>	Live corridor traffic heatmap (from vendor ATCC/VIDES feed), active incidents with SLA timers, device health per project, weather alerts, enforcement activity, inter-corridor comparison, Road condition.
<b>LCCC Operator Dashboard</b>	Active incident queue (severity + SLA countdown), device fault alerts, SOP task queue, weather threshold alerts, VMS advisory status (from vendor platform), shift statistics.
<b>KPI Framework Dashboard</b>	Configurable KPI tiles with RAG colour coding; drill-down to underlying data; historical trend charts 1hr–5yr range; ITIL/BPMN workflow configuration.
<b>SLA Dashboard</b>	Contract-level and device-level SLA compliance, penalty computation, dispute evidence packages. All SLA data auto-computed and digitally timestamped. Accessible to IHMCL and TSPs.
<b>Contractor / TSP Portal</b>	Read-only SLA metrics, device availability, open maintenance tickets, penalty computations for TSP contract scope only.

#### 7.10.1. National Dashboard

The National Dashboard provides MoRTH, IHMCL, and NHAI leadership with a real-time and historical view of national highway performance across all ATMS corridors. Key performance indicators displayed include: national incident rate, average incident clearance time, enforcement actions per day, FASTag compliance rate, system-wide device availability, and SLA breach statistics by contractor.

#### 7.10.2. Regional Dashboard

Each Regional Command Centre has a region-specific dashboard providing operational situational awareness for the zone director and operators. The dashboard includes: live corridor traffic heatmap, active incidents list with SLA timers, device health summary by project, weather alerts, and daily/weekly/monthly performance trend charts.



---

### 7.10.3. Local Dashboard

Technology Service Providers are provided with a dedicated contractor portal showing their SLA performance metrics, device availability by project, open maintenance tickets, upcoming planned maintenance schedules, and penalty liability status. The portal is read-only and provides TSPs with transparent visibility into the automated SLA computation.

### 7.10.4. SLA Dashboard

The SLA Dashboard is the authoritative reporting interface for IHMCL and NHAI's contract management team. It provides contract-level and device-level SLA compliance data, performance trend analysis, penalty computation, and dispute evidence packages. All SLA data is computed automatically from system telemetry and is timestamped and digitally signed to serve as evidence in contract disputes.

## 7.11. Platform DevOps & CI/CD Environment Architecture

The SDA shall design, implement, and maintain a complete DevOps infrastructure supporting the full software delivery lifecycle:

- CI/CD Pipelines: Automated build, unit test, SAST/DAST security scan, container image build, and Kubernetes deployment for all platform services. Zero-downtime rolling deployments with automated rollback.
- Infrastructure-as-Code (IaC): All cloud infrastructure provisioned via Terraform/Ansible or equivalent. IaC codebase version-controlled in Git; all changes peer-reviewed and audit-logged.
- Environments: Development, Staging/UAT, Production, and DR — each with its own namespace in the MEITY GCC or On-premises Kubernetes cluster.
- Observability Stack: Centralised logging (ELK/OpenSearch), distributed tracing (Jaeger/Zipkin), APM dashboards (Grafana/Prometheus). All services instrumented from Day 1.
- Release Governance: Quarterly minor releases and annual major releases. Change management via formal Change Advisory Board (CAB) review. Release notes, version tagging, and deployment audit trail mandatory.
- SBOM (Software Bill of Materials): Maintained for all platform components; scanned against NVD on every deployment.

## 7.12. OEM Vendor Sandbox Environment

The SDA shall establish and maintain a perpetually available Sandbox Environment enabling any Registered OEM Vendor to test their field devices, sensors, cameras, ANPR systems, and other ATMS hardware against the ATMS Platform APIs before field deployment. The Sandbox shall include:

- A complete replica of the ATMS Platform API gateway with full API documentation (OpenAPI 3.0)
- A software test harness simulating NCCC/RCCC/LCCC environments
- Simulated data ingestion pipelines for events, ANPR, sensor data, and video analytics results
- OEM registration portal for self-service sandbox access with API key management
- Test result dashboards showing integration health, message throughput, and error logs

- Documentation: integration guides, device onboarding manuals, protocol specifications

The Sandbox shall be available 24x7 with minimum 99% uptime. IHMCL may add new OEMs to the registration list at any time during the contract period. The IA shall provide technical support to OEM vendors for integration queries within 2 business days.

### 7.13. Integrated Audio Communication Engine

The Integrated Audio Communication Engine enables Traffic Managers and operators to communicate with all highway stakeholders, ambulance services, trauma centres, police PCR, highway patrol (RPV), crane operators, highway maintenance, and NHAI officials across all communication media from a single workstation.

#### 7.13.1. Architecture

- SIP/VoIP Core: Software-defined IP PBX (Asterisk, FreeSWITCH, or equivalent enterprise telephony platform) supporting SIP trunks for PSTN/GSM, VoIP extensions, and ECB/1033 integration.
- Media Gateway: Interfaces between PSTN landline, GSM/mobile radio (UHF/VHF via radio-over-IP gateway), VoIP, and roadside ECB/ERT systems.
- Call Recording Engine: All calls recorded in real time at the SIP/RTP layer; recordings archived to WORM-protected object storage with AES-256 encryption; tamper-evident digital signature at capture.
- Context-Sensitive Dialling Engine: SOP workflow engine triggers auto-dial to configured stakeholder on SOP task click; stakeholder contacts resolved from the ATMS Contacts Directory.
- Conference Bridge: Up to 9-party conference with add/remove mid-call; group broadcast to all patrol units in a jurisdiction.
- In-Platform Messaging: WebSocket-based real-time text messaging between operators across all tiers; 1-year message history; incident-scoped collaboration threads for Major+ incidents.

#### 7.13.2. Key Technical Specifications

<b>Call Recording Retention</b>	Minimum 30 days (all calls); 10 year minimum for calls linked to closed incident records; WORM storage; immutable post-capture
<b>Concurrent Calls</b>	Up to 9 simultaneous calls per workstation; no per-LCCC limit on concurrent sessions across the platform
<b>Disconnection Control</b>	Disconnect prohibited until call is answered; on-screen prompt required before ending any call linked to Catastrophic incident
<b>Call Quality Monitoring</b>	Real-time MOS score, packet loss, jitter monitoring; alert if quality falls below configured threshold; historical data for SLA assessment
<b>ECB Integration</b>	ECB calls routed to LCCC operator via 1033 helpline SIP trunk; auto-identification of ECB ID and KP from caller-ID mapping table

### 7.14. Report Generation and Analytics Engine

The analytics engine processes ATMS-native data and vendor feed data to produce operational dashboards, automated reports, and ad-hoc analytics.

#### 7.14.1. Architecture

- Reporting Database: Dedicated read-replica PostgreSQL or columnar database or similar (Apache Doris / ClickHouse or equivalent) pre-optimised for analytical queries; separate from the operational OLTP database.
- Report Scheduler: Apache Airflow or equivalent workflow orchestrator for automated report generation and email distribution on daily/weekly/monthly/quarterly schedules.
- BI/Visualisation Layer: Grafana, Apache Superset, or equivalent open-source BI platform; embedded in the ATMS GUI via i-frame or native integration. All charts interactive with drill-down.
- KPI Engine: Rules-based KPI computation engine; administrators define KPI formula, thresholds, and reporting frequency without coding. Results written to KPI dashboard tables every 5 minutes.
- Ad-Hoc Query Builder: SQL-free guided query interface for Data Analysts; results visualisable or exportable as CSV. Multi filter query interface for Data Dashboards or Reports.
- Report Export Service: PDF generation via headless browser rendering; Excel (XLSX) export via Apache POI or equivalent; CSV export direct from database. All PDF exports watermarked with user ID and export timestamp.

#### 7.14.2. Pre-Built Report Library — Summary

Report Name	Frequency	Data Sources
Daily Operations Summary (per LCCC/RCCC/NCCC)	Daily — 00:00 IST	ATMS IPE, DAQ, vendor feeds, AWS
Weekly Enforcement Revenue	Weekly	Vendor e-Challan feed + NIC portal
Monthly SLA Performance (per TSP/project)	Monthly	ATMS NMS + vendor NMS telemetry
Annual Programme Performance (for MoRTH/NHAI)	Annual	All ATMS modules + vendor feeds
Shift Handover Report	Per shift change	ATMS IPE, SLA engine, NMS, DAQ
NHAI ATMS Policy Chapter 7 Compliance Dashboard	Monthly	All ATMS KPIs vs Policy targets
CERT-In Cybersecurity Compliance Report	On-demand	SIEM, IAM, patch management logs
Incident Hotspot Analysis	Monthly	ATMS IPE + weather + ATCC (vendor feed)

---

### 7.15. Mobile Application Stack

Native mobile app for iOS (v16+) and Android (v12+) for field maintenance staff and highway patrol officers.

#### 7.15.1. Architecture

- Front-End: React Native (cross-platform) or native Swift/Kotlin for performance-sensitive functions. Offline-first architecture using SQLite local cache with automatic cloud sync on reconnection.
- Backend: Java/ NodeJS / PHP Laravel for mobile backend and APIs, based on overall selection of backend for the web applications.
- Authentication: Same MFA-enforced OAuth 2.0 SSO as desktop interface; biometric unlock after initial MFA login per session.
- Push Notifications: Firebase Cloud Messaging (FCM) / Apple Push Notification Service (APNS) for real-time alerts (incident assignments, watch-list hits near officer GPS location from vendor ANPR feed, broadcast messages).
- GPS Location Reporting: AIS-140 compatible GNSS location updates published to ATMS via MQTT every 30 seconds; makes patrol vehicles visible on NCCC/RCCC/LCCC GIS maps.
- Offline Sync Engine: All assigned tickets and incident data cached locally; all offline actions queued with timestamp; sync in chronological order on reconnection.
- CCTV Stream View: Stream tokens received from vendor TMCS platform via ATMS API gateway; displayed in mobile video player; quality auto-adjusts to available bandwidth.

### 7.16. Alarm Management Engine

Centralised, real-time alarm presentation and management across all operator workstations.

#### 7.16.1. Architecture

- Alarm Bus: Kafka-backed real-time alarm event stream; alarm records persisted to PostgreSQL with full lifecycle audit trail.
- Priority Engine: Configurable rule-based priority scoring engine using: alarm type weight, geographic location criticality, device type severity, SLA impact score, and time-elapsed since generation.
- Alarm Correlation: Sliding-window correlation (default: 5-minute, 500m radius) groups related alarms from multiple sources into a single correlated alarm event — prevents flooding.
- Alarm Sources: ATMS-native (device health faults, SLA breaches, weather threshold breaches, cybersecurity events) AND structured alarm events from Existing Field Platform Vendor (VIDES detection events, ANPR watch-list hits, VMS device faults).
- Notification Delivery: Visual pop-ups (WebSocket push to browser), audible tones (configurable per category), SMS (Twilio/MSG91/Other gateway), email via SMTP.
- Alarm Audit Store: All alarm actions (acknowledge, assign, suppress, close) logged with timestamp, user ID, action, and notes; WORM-protected; 5-year retention.

---

### 7.17. Road User Information Platform

Public-facing web and mobile application providing real-time highway information — no registration required for general access.

#### 7.17.1. Architecture

- Public API Layer: A separate, read-only API gateway serving the public road user interface; isolated from the operational ATMS API gateway; rate-limited at 100 requests/min per IP.
- Front-End: Progressive Web App (PWA) — works on all browsers without app install. Native iOS and Android apps also published (React Native).
- Map Engine: Same OpenLayers/Mapbox GL JS as operational GIS but with a public-optimised tile caching layer (CDN-backed) for high-volume concurrent user handling.
- Data Sources: Traffic speed (from vendor ATCC/VIDES/ANPR data), active incidents (from ATMS IPE), weather (from ATMS AWS + IMD), VMS messages (from vendor VMS platform) — all read-only, no operational data modified.
- Push Notifications: Opt-in corridor-specific alerts via FCM/APNS; configurable by road users for incident types, weather, road works.
- Rajmarg/NHAI App Integration: Real-time feed via MoRTH open data standard REST API; geo-tagged advisory push; event closure notifications.

### 7.18. Multi-Source Data Fusion Engine

Aggregates and correlates intelligence from all sources — ATMS-native, vendor feeds, crowd-sourced, and social media to generate actionable operational intelligence.

#### 7.18.1. Architecture

- Social Media Ingestion: Scheduled API polling of Twitter/X and Facebook for highway-related posts in Indian languages; configurable RSS/news feeds. Rate-limited to avoid API ban; cached per 15-minute windows.
- NLP Processing Engine: Apache Spark NLP or Hugging Face Transformers (hosted within on-premises ATMS infrastructure) for: incident type extraction, location entity recognition, severity classification, and operational relevance scoring from Indian-language social media posts.
- Correlation Engine: Cross-source event correlation using: geo-proximity (configurable radius), temporal window (default: 15 minutes), and semantic similarity (NLP-based). Correlation matches presented to operator for confirmation before SOP trigger.
- Intelligence Dashboard Feed: WebSocket-pushed real-time intelligence feed in the operator GUI; scoped to user's tier and jurisdiction; configurable filter by source type, confidence threshold, and event type.
- SOP Auto-Trigger: On reaching configurable minimum correlation confidence threshold (default: 0.8), engine auto-recommends or triggers the appropriate SOP via the IPE SOP workflow engine.

---

### 7.19. Weather and Environmental Monitoring Engine

Direct acquisition and processing of ATMS-managed AWS sensor data and IMD forecast data.

#### 7.19.1. Architecture

- AWS Ingestion: MQTT-based data ingestion from roadside Automatic Weather Stations (ATMS-managed hardware); default 5-minute interval; all 9 parameters (temperature, humidity, rainfall, wind speed/direction, visibility, road surface temperature, road surface condition).
- IMD Integration: RESTful API polling of IMD national forecast data every 3 hours; geo-matched to ATMS corridor KP references for corridor-level forecast display. IMD data will be integrated into Road User Applications and other telecom and third party aggregator apps to warn road users under certain scenarios.
- Threshold Alert Engine: Rule-based real-time evaluation of all AWS readings against configurable thresholds (visibility <200m, road surface icy/flooded, wind >60 km/h, rainfall >20mm/hr). Threshold breach generates: (a) ATMS alarm; (b) VMS advisory request to vendor API; (c) IMD-correlated weather alert on GIS map.
- Weather-VMS Audit Chain: Every automated VMS advisory request triggered by weather is logged with: triggering AWS ID, parameter breached, measured value, ATMS request timestamp, and vendor VMS ACK timestamp. Full audit chain from weather condition to advisory.
- Historical Weather Store: All AWS data retained 10 years in national data lake; accessible via analytics API for climate-incident research.

### 7.20. ATMS Engine Invocation Summary

The attached matrix outlines the specific functional roles of various software engines across three operational tiers: the Local Command & Control Centre (LCC), Regional Command & control Centre (RCC), and National Command & control Centre (NCCC). It details how ten core systems—including Event Processing (EPE), Incident Processing (IPE), GIS, and Security (SIEM/IAM)—scale their capabilities from the ground up. At the LCCC level, these engines focus on localized data ingestion, edge processing, and immediate incident response. Moving to the RCC, the focus shifts to aggregating that data for regional correlation, cross-corridor coordination, and broader performance tracking. Finally, at the NCCC level, the engines handle massive-scale operations, national executive dashboards, centralized analytics, and major cross-agency integration.

ENGINE	LCC — Local Control Centre	RCC — Regional Command Centre	NCC — National Command Centre
<b>FRS Ref</b>			
<b>EPE — Event Processing Engine</b> FR-DAQ-001..010	All field device events, AWS/ECB data, VIDES/ANPR/VMS vendor feeds ingested at LCC edge; events published to Kafka; deduplication of multi-	Regional EPE aggregates LCC event streams; applies regional correlation rules; routes to IPE for escalation	NCC EPE processes all national event streams; 100K+ events/sec; feeds national data lake; routes to SIEM, DL, analytics
<b>IPE — Incident Processing Engine</b> FR-INCD-001..025	Incident lifecycle owner at LCC: Detected→Confirmed→Dispatched→Cleared→Closed. SOP orchestration, SLA timer tracking, iCAD dispatch	Receives escalated incidents from LCC; RCC supervisor takeover; cross-LCC coordination; one-click NCC escalation	National incident overview; Catastrophic incident command; NERS 112 auto-notify; DMC/SDMA push within 2 min
<b>GIS — National GIS Platform</b> FR-HTM-001..026	Full-detail corridor map; 18 device layers; video wall tiling (stream tokens); strip chart view; map-click incident creation; LCC COP	Regional map covering all LCC corridors; inter-corridor comparison overlay; traffic speed layer; patrol GPS tracking	National map all RCC regions; aggregate metrics per region tiles; executive COP; PM Gati Shakti integration
<b>DCE — Command Dispatch Engine</b> FR-SOP-009, FR-INT	VMS advisory request →VASD API; PTZ advisory →TMCS API; 1033 iCAD dispatch; NERS 112 notify from LCC-confirmed Major incidents	Regional VMS advisory campaigns; cross-LCC emergency commands; state ICC event push	National broadcast commands; DMC/SDMA push; Police PCR stream token provisioning; DATEX II feed
<b>AUD — Audio Communication Engine</b> FR-AUD-001..017	Primary tier for audio, 1033/ECB calls; SOP auto-dial to stakeholders; up to 9 concurrent calls; WORM call recording	RCC conference calls bridging multiple LCC operators and agencies; broadcast to all LCC operators in region	National broadcast voice advisory to all RCC/LCC supervisors; senior leadership conference bridges
<b>NMS — Network Management System</b> FR-NMS-001..021	LCC-scope device monitoring: AWS, ECBs, routers, switches, edge servers; fault-to-ticket automation; 60-sec alert on fault	Regional aggregation of LCC NMS data + vendor NMS telemetry; TSP SLA computation per corridor/region	National device health heatmap; programme-level SLA; financial penalty computation; Contractor Portal management
<b>RPT — Report &amp; Analytics Engine</b> FR-RPT-001..020	Daily operations summary; shift handover report; LCC corridor performance dashboard	Regional weekly/monthly SLA performance; inter-corridor comparison; TSP penalty reports; PIU/RO portal	Annual programme report (MoRTH/NHAI); national KPI dashboard; AI prediction outputs; DataLake API push
<b>SIEM / IAM — Security Engines</b> FR-SEC-001..014	RBAC enforcement; session timeout; MFA on all logins; audit log forwarding to NCC SIEM	Regional access control; jurisdictional data scoping; access-denied SIEM alerts	Central SIEM 24x7 CSOC; UEBA anomaly detection; CERT-In reporting; annual VAPT coordination; PAM/JIT access
<b>VDIL — Vendor Data Interface Layer</b> FR-INT-016..021	Receives VIDES incident events, ANPR/TTMS data, VMS status, ATCC traffic data from vendor platform instances per corridor	Aggregates vendor feeds across region; feed health monitoring per LCC corridor	Manages all vendor API connections; global VDIL health dashboard; schema version control; DES compliance
<b>ALM — Alarm Management Engine</b> FR-ALM-001..008	Receives alarms from ATMS-native sources + vendor feeds (VIDES detections, ANPR watch-list hits, VMS faults). Operator: Ack/Assign/Suppress	Regional alarm priority queue; cross-LCC alarm correlation; SLA-impact ranked alarms for RCC supervisor	National critical condition warnings; programme-level alarm KPIs; cybersecurity alarm routing to CSOC

Figure 19: ATMS Engine Invocation: Which Engine Fires at each Tier



## 8. WORK PACKAGES AND ITS DELIVERABLES

### 8.1. WORK PACKAGE -1 SCOPE SUMMARY AND KEY DELIVERABLES (YEARS 1 – 5)

The following deliverables shall be produced under Work Package 1:

Deliv. ID	Deliverable Name	Description
WP1-D01	Operational ATMS Core Platform	All FRS modules as per RFP are deployed at LCCC, RCCC and NCCC (On premises DC and Cloud DR). Additional modules may be added based on project/policy requirements during project tenure.
WP1-D02	GIS-Based COP Dashboards	National, regional, and corridor-level GIS dashboards providing real-time COP with all configurable ITS device layers, incident layer, traffic speed layer, and weather layer
WP1-D03	External System Integration Interfaces	All external government/agency integrations operational and acceptance-tested: VAHAN, SARATHI, FASTag/NETC, CCTNS, iCAD, Rajmarg, NHAI App, NERS 112, eCourts, IMD, DMC/SDMA, State ICCCs, Police PCR, AIS-140, DigiLocker, PM Gati Shakti, IHMCL DataLake, NIC Enforcement Portal. Additional integrations may be required as per project requirements during project tenure.
WP1-D04	Vendor Data Interface Layer (VDIL)	All Existing Field Platform Vendor API interfaces (VIDES, ANPR/TTMS, VMS, Radar, VASD, enforcement/e-Challan, Vendor NMS, ATCC) operational per DES; Data Exchange Specification signed by all three parties
WP1-D05	National Data Lake & Analytics Framework	Three-zone data lake (Bronze/Silver/Gold), predictive analytics models, KPI engine, report scheduler, and BI/visualisation layer operational
WP1-D06	Cybersecurity Stack	IAM, MFA, ZTA, SIEM (CERT-In compliant), EDR, IDS/IPS, DLP, PAM, NAC, network micro-segmentation, encryption, audit logging — all operational at NCCC/RCCC/LCCC
WP1-D07	Integrated Audio Communication System	Full Integrated Audio Communication Engine (Section 5.12) operational — ECB/1033 integration, call recording, in-platform messaging, PTT/radio integration
WP1-D08	Mobile Application	iOS and Android field operator app (Section 5.14) published and operational
WP1-D09	Road User Information System	Progressive web app with externally published APIs for third party sites to showcase road information (as per Section 7.17)

Deliv. ID	Deliverable Name	Description
WP1-D10	Weather & Environmental Monitoring Engine	Data Fusion and alerts engine functional and operational (as per Section 7.18)
WP1-D11	Validated Production Platform	Full-scale performance validated (100K+ devices, 10M+ vehicles/day); DR test passed (RTO<2hr, RPO<4hr); initial VAPT cleared
WP1-D12	DevOps, IaC & Sandbox Environment and O&M	CI/CD pipelines, IaC codebase, observability stack, and OEM sandbox environment operational and Software Operation & Maintenance
WP1-D13	Programme Governance & Release Framework	PMO, change management process, release cadence, SRS baseline, RTM, SBOM, and all required project documentation

## 8.2. WORK PACKAGE 2: SOFTWARE ENHANCEMENTS & PRODUCT EVOLUTION (YEARS 6–10)

### 8.2.1. Enhancement Team Composition (Years 6–10)

The IA shall maintain a dedicated Enhancement Team throughout Years 6–10 as follows:

Role	Years 6–8 (Man-Months/Year)	Years 9–10 (Man-Months/Year)	Notes
Solution Architect	6	4	Platform evolution guidance; technology refresh planning
Senior Developers	12	9	Feature development, AI model retraining, critical patches
Software Developers	18	12	Feature development, new integrations, regulatory updates
Integration / DevOps Engineers	6	4	New API integrations; CI/CD pipeline maintenance
Data Analyst / ML Engineer	9	6	Analytics enhancements; AI model retraining cycles
QA Automation Engineer	6	4	Regression testing; performance testing; VAPT preparation

### 8.2.2. Scope of Software Enhancements

- Feature Enhancements: Annual major releases and quarterly minor releases based on operational feedback from NCCC, RCCC, and LCCC teams

- Integration Expansion: New highway systems, sensors, enforcement platforms, and state ICCC integrations
- Analytics and Reporting Enhancements: New KPI dashboards, enhanced predictive analytics, self-service analytics for IHMCL management
- AI and Detection Model Improvements: AI and Predictive Model Improvements: Bi-annual retraining of ATMS-native congestion prediction and incident risk prediction models; improved forecast accuracy; weather-incident correlation model updates. ANPR accuracy and violation detection improvements remain with the Existing Field Platform Vendor.
- Technology Upgrades: Framework updates, EOL component elimination, security patch management (Critical: 72 hrs; High: 14 days)
- Regulatory and Policy Updates: DPDP Act compliance, CERT-In directive implementation, NHAI ATMS Policy evolution
- Cloud Platform and Observability Enhancements: Annual cost optimization, scalability framework updates, cloud service migrations

### 8.2.3. WP-2 Key Deliverables

Deliverable ID	Deliverable Name	Frequency
WP2-D01	Periodic Platform Feature Releases	Minimum quarterly release cycle
WP2-D02	New System Integration Modules	Per Enhancement Order; as new systems are on-boarded
WP2-D03	DevOps and Platform Observability Framework Updates	Continuous; major updates quarterly
WP2-D04	Enhanced Analytics and Monitoring Tools	Per Enhancement Order; minimum annually
WP2-D05	AI and Event Detection Model Updates	Minimum biannual model retraining and release
WP2-D06	Technology Upgrade Release Packages	Minimum annual; critical patches on-demand
WP2-D07	Policy and Compliance Update Packages	As required by regulatory changes
WP2-D08	Annual Enhancement Programme Report	Annual; submitted by January each year for IHMCL review

### 8.3. WORK PACKAGE 3: DEPLOYMENT & CORRIDOR INTEGRATIONS (YEARS 1–10)

**8.3.1. Deployment Team Composition (Years 1–10)**

The SDA shall maintain a dedicated Deployment and Integration Team throughout the contract:

Role	Y1–3 (MM/Yr)	Y4–5 (MM/Yr)	Y6–8 (MM/Yr)	Y9–10 (MM/Yr)
Deployment / Integration Architect	12	6–9	4	2
Deployment / Integration / DevOps Engineers	24	18	12	6
Data Integration / Analytics Engineer	9	9	6	3
System Test and Validation Engineer	9	9	6	3

**8.3.2. Phased Rollout Schedule**

Deployment Phase	Period	Scope	Milestone
Phase 1 — NCCC + Pilot	Year 1 (M9–M12)	NCCC deployment; 1 RCCC pilot; 10 LCCC pilot sites	NCCC Go-Live (MS-07)
Phase 2 — Wave 1	Year 2 (M1–M12)	2 full RCCCs + 150 LCCCs commissioned	Wave 1 SAT (MS-09)
Phase 3 — Wave 2	Year 3 (M1–M12)	All 10 RCCCs + 250 LCCCs commissioned	Wave 2 SAT / System Acceptance Certificate
Scale-Up Phase 1	Years 4–8	New corridors as NHAI expands; up to 250 LCCs and 20 RCCCs	Per-corridor SAT (WP3-06 trigger)
Completion Phase	Years 9–10	Final 167 LCCCs onboarded to reach 667 target; WP-3 closes on last SAT	Final Corridor Commissioning Certificate

**8.3.3. Per-Corridor Onboarding Activities**

Each corridor onboarding covers the following activities:

- Secure communication channel establishment: Managed MPLS redundant connectivity for each new LCCC (To be provided by IHMCL). IHMCL shall intimate SDA when the LCCC site is ready for onboarding for deployment of LCCC ATMS software.
- MQTT broker configuration: topic hierarchy setup, certificate provisioning, message schema validation rules

- Vendor VDIL configuration: VIDES event feed, ANPR/TTMS data feed, VMS status feed, and vendor NMS telemetry configured per DES for the new corridor's vendor platform instance
- GIS update: New corridor highway network loaded, KP reference calibrated, POI database updated, device icons provisioned
- Device onboarding pipeline: All new ATMS-managed devices (TMCS, VIDES, ANPR, VASD, AWS, ECBs, network equipment etc.) registered, certificates issued, heartbeat monitoring active
- End-to-end data flow validation: Bronze zone ingestion confirmed for all data types
- Corridor SAT (Site Acceptance Test): Functional test of all applicable FRS requirements at corridor level; IHMCL sign-off
- Operator training: Initial operator training for LCCC staff (per WP-5 training programme)

#### 8.4. Work Package 4 — Operations and Maintenance (Years 2–10)

WP-4 covers all operations and maintenance services from the end of Year 1 through Year 10. O&M staffing is structured in three profiles reflecting the maturity of the deployed platform:

- Years 2–3: Full O&M team — peak staffing during active deployment and stabilisation.
- Years 4–7: Adjusted profile — steady-state O&M with right-sized team.
- Years 8–10: Reduced profile — mature platform with lower routine O&M effort.

WP4-04 (Annual DR Test) is priced separately and covers a full DC-to-DR failover simulation each year, validating RTO < 4 hours and RPO < 2 hours. All rates are exclusive of GST.

##### 8.4.1. WP-4 Bill of Quantities — Operations and Maintenance

BoQ Item	Description	Unit	Qty (Indicative)
WP4-01	O&M Service — Years 2–3: Full O&M team Includes: Full NOC staffing (24×7 L1/L2/L3); field operations team; system administration; incident management; performance monitoring; monthly SLA reports; helpdesk operations; preventive maintenance scheduling; all tools and licences for O&M platform.	Per Year	2
WP4-02	O&M Service — Years 4–7: Adjusted profile Includes: All WP4-01 scope with right-sized team for steady-state platform operations. Reduced onboarding-related effort; stable ATMS platform; NOC staffing adjusted per agreed SLA matrix.	Per Year	4
WP4-03	O&M Service — Years 8–10: Reduced profile Includes: All WP4-02 scope with further adjusted team for mature platform. Emphasis on preventive	Per Year	3

BoQ Item	Description	Unit	Qty (Indicative)
	maintenance, SLA compliance, technology obsolescence management, and transition preparation for Contract renewal or expiry.		
WP4-04	Annual DR Test — Full failover simulation, RTO/RPO validation Includes: Annual full DC-to-DR failover simulation; RTO validation (target < 4 hours); RPO validation (target < 2 hours); test report with detailed timings for each system component; remediation plan if targets are missed; IHMCL sign-off on DR Test Report.	Per Year	9

#### 8.4.2. Staffing Summary — All Periods

Location tier / Team	Yrs 2–3 (Full)	Yrs 4–7 (Adjusted)	Yrs 8–10 (Reduced)	Primary driver of change between periods
A — NCCC Platform Support	11	8	4	Platform stabilises
B — RCCC Application Support	5	5	4	Stable from Year 3; slight consolidation in Years 5–10 as platform matures
C — LCCC Field Technical Support	8	13	12	Scales with live corridor count (avg 135 → 540 → 667); matures — ratio improves
D — Programme Management & Quality	2	2	1	
<b>TOTAL FTEs</b>	<b>26</b>	<b>28</b>	<b>21</b>	

#### 8.4.3. LCCC Coverage Ratio — Technical Support per Active Corridor

Period	Active LCCCs (average)	LCCC Technical Engineers	Coverage ratio	Rationale
Years 2–3 — Full	~135 (ramping 10 → 261)	8	1 per ~25 LCCCs	New sites have high issue rate; frequent on-site visits during commissioning period
Years 4–7 — Adjusted	~540 (ramping 411 → 667)	13	1 per ~42 LCCCs	Platform stabilising; majority of issues resolved remotely; visits for hardware-software faults only
Years 8–10 — Reduced	667 (all live)	12	1 per ~56 LCCCs	Mature platform; automation and remote tooling reduce ticket volume per site; focus on patch compliance and exit docs

#### 8.4.4. Years 2–3 — Technical Support Staffing Detail

Total technical support staff: 26 | Full O&M — stabilisation, new corridor onboarding, high issue rate

Role / Position	FTEs	Application / system support scope and responsibilities
<b>NCCC — Central ATMS Platform</b> <i>Application and technical support for the central ATMS platform, data lake, analytics engine, integration interfaces (VDIL and external government systems), cybersecurity stack.</i>		
Application Support Lead — ATMS Core	1	Overall central platform health; vendor SLA management; L3 escalation authority; release coordination
Application Support Engineers — ATMS Core	2	Bug triage; patch deployment; configuration management; testing for core ATMS platform modules
Application Engineers — Analytics, BI & Data Lake	2	Bronze/Silver/Gold zone pipeline support; KPI engine; BI/reporting layer; data quality monitoring
Integration / API Engineers — VDIL & External APIs	3	VDIL feed support (VIDES, ANPR, VMS, Radar, VASD, Vendor NMS); external API health (VAHAN, SARATHI, FASTag, CCTNS, NERS, etc.); DES compliance
Database Administrators (DBA)	2	Central database health; query optimisation; backup validation; capacity management; DC-to-DR database replication health



Role / Position	FTEs	Application / system support scope and responsibilities
Security / Cybersecurity Engineer	1	Cybersecurity stack (IAM, MFA, ZTA, SIEM, EDR, IDS/IPS); VAPT cycle coordination; CERT-In compliance; access rights reviews
<b>Sub-total — NCCC</b>	<b>11</b>	<i>Full central team to support stabilisation of the core platform, active VDIL onboarding, and high volume of new integration commissioning.</i>
<b>RCCC — Regional Control Centres (10 locations)</b> <i>Application and technical support for the regional ATMS software instance, local servers, operator workstations, and site-specific integrations installed at each of the 10 RCCCs. Support staff are centrally based and travel to RCCC sites as needed (planned monthly visits in Years 2–3; quarterly in Years 4+).</i>		
RCCC Application / Technical Engineers	5	Application support for regional ATMS instance; local server and workstation health; site-specific integration configuration; operator issue triage and resolution; planned monthly site visits to each RCCC; remote support between visits
<b>Sub-total — RCCC</b>	<b>5</b>	<i>10 RCCCs live by end of Year 3. Each engineer supports 2 RCCCs — monthly planned site visit + remote support for application and infrastructure issues.</i>
<b>LCCC — Local Corridor Control Centres (up to 667 corridors)</b> <i>Field technical support for ATMS software agents, edge software, and hardware installed at each LCCC corridor. Covers ATMS agent health, edge device application configuration, software patches, and planned or corrective on-site technical visits. Most support is delivered remotely; on-site visits are for issues that cannot be resolved remotely.</i>		
LCCC Field Technical Engineers	8	ATMS software agent health and configuration; edge software patch deployment; device application configuration; remote diagnostics; on-site corrective technical visits; new corridor commissioning support alongside WP3 team; documentation of as-installed configuration per site
<b>Sub-total — LCCC</b>	<b>8</b>	<i>~10 to 261 LCCCs live during Years 2–3 (average ~135 active). High issue rate on newly commissioned sites. Coverage ratio: 1 engineer per ~25 active LCCCs. Engineers are geographically clustered to minimise travel time.</i>
<b>Programme Management &amp; Quality</b> <i>O&amp;M programme governance, quality assurance, patch testing, release coordination, and compliance management across all location tiers.</i>		
O&M Programme Manager	1	Overall O&M delivery; SLA governance across all tiers; IHMCL interface; monthly reporting; Change Advisory Board; vendor management

Role / Position	FTEs	Application / system support scope and responsibilities
Quality & Testing Engineer	1	Patch validation testing before deployment; regression suites; DR test participation; test-case library maintenance
<b>Sub-total — Programme Management &amp; Quality</b>	<b>2</b>	
<b>GRAND TOTAL — Years 2–3</b>	<b>26</b>	

#### 8.4.5. Years 4–7 — Technical Support Staffing Detail

Total technical support staff: 28 | Adjusted O&M — steady state, scale-up, platform maturing

Role / Position	FTEs	Application / system support scope and responsibilities
<b>NCCC — Central ATMS Platform</b> <i>Application and technical support for the central ATMS platform, data lake, analytics engine, integration interfaces (VDIL and external government systems), cybersecurity stack installed at the NCCC.</i>		
Application Support Lead — ATMS Core	1	Platform health; vendor liaison; L3 escalation; release governance
Application Support Engineers — ATMS Core	2	Bug triage; patch deployment; configuration management
Application Engineer — Analytics & Data Lake	1	Pipeline support (reduced effort as pipeline stabilises); BI and reporting layer
Integration / API Engineers — VDIL & External	2	VDIL feed maintenance; new state ICCC integrations (per WP3 scale-up); external API health
Database Administrator (DBA)	1	DB health; capacity; backup validation; replication monitoring
Security / Cybersecurity Engineer	1	SIEM monitoring; VAPT cycle; compliance; access audit
<b>Sub-total — NCCC</b>	<b>8</b>	<i>Platform stabilises. Integration engineers reduce as VDIL connections mature.</i>

Role / Position	FTEs	Application / system support scope and responsibilities
<b>RCCC — Regional Control Centres (20 locations)</b> <i>Application and technical support for the regional ATMS software instance, local servers, operator workstations, and site-specific integrations installed at each of the 20 RCCCs. Support staff are centrally based and travel to RCCC sites as needed (planned monthly visits in Years 2–3; quarterly in Years 4+).</i>		
RCCC Application / Technical Engineers	5	Regional ATMS instance support; server/workstation health; patch deployment; local integration configuration; quarterly planned site visits; remote resolution for most issues
<b>Sub-total — RCCC</b>	<b>5</b>	<i>All 20 RCCCs fully live. Support profile stable — 1 engineer per 4 RCCCs. Quarterly planned visits replace monthly as platform matures.</i>
<b>LCCC — Local Corridor Control Centres (up to 667 corridors)</b> <i>Field technical support for ATMS software agents, edge software, and installation at each LCCC corridor. Covers ATMS agent health, edge device application configuration, software patches, and planned or corrective on-site technical visits. Most support is delivered remotely; on-site visits are for issues that cannot be resolved remotely.</i>		
LCCC Field Technical Engineers	13	ATMS agent application support; edge software and configuration management; remote diagnostics (primary resolution mode); on-site visits for hardware-software faults; new corridor onboarding support as WP3 scale-up continues; monthly patch compliance verification
<b>Sub-total — LCCC</b>	<b>13</b>	<i>411 to 667 LCCCs progressively live (average ~540 active). Support volume scales with corridor count. Coverage ratio: 1 engineer per ~42 active LCCCs. Platform stabilising — majority of issues resolved remotely; site visits for hardware-software faults only.</i>
<b>Programme Management &amp; Quality</b> <i>O&amp;M programme governance, quality assurance, patch testing, release coordination, and compliance management across all location tiers.</i>		
O&M Programme Manager	1	O&M delivery; SLA governance; IHMCL interface; reporting; change advisory
Quality & Testing Engineer	1	Patch validation; regression testing; DR test; compliance test execution
<b>Sub-total — Programme Management &amp; Quality</b>	<b>2</b>	

Role / Position	FTEs	Application / system support scope and responsibilities
<b>GRAND TOTAL — Years 4–7</b>	<b>28</b>	

**8.4.6. Years 8–10 — Technical Support Staffing Detail**

Total technical support staff: 21 | Reduced O&M — mature platform, exit readiness, handover preparation

Role / Position	FTEs	Application / system support scope and responsibilities
<b>NCCC — Central ATMS Platform</b> <i>Application and technical support for the central ATMS platform, data lake, analytics engine, integration interfaces (VDIL and external government systems), cybersecurity stack at the NCCC.</i>		
Application Support Engineers — ATMS Core	1	Platform stability; critical security patches; technology refresh support; exit handover documentation
Integration / API Engineer	1	VDIL and external interface maintenance; new integrations winding down
Database Administrator (DBA)	1	DB health; data archival strategy; exit handover — data migration preparation
Security / Cybersecurity Engineer	1	SIEM; annual VAPT coordination; exit compliance documentation
<b>Sub-total — NCCC</b>	<b>4</b>	<i>Mature platform. Focus shifts to patch compliance, Year 9 technology refresh, and exit handover documentation.</i>
<b>RCCC — Regional Control Centres (20 locations)</b> <i>Application and technical support for the regional ATMS software instance, and site-specific integrations installed at each of the 20 RCCCs. Support staff are centrally based and travel to RCCC sites as needed.</i>		
RCCC Application / Technical Engineers	4	Application and infrastructure support; patch deployment; exit handover — RCCC configuration documentation, credentials, and as-installed records
<b>Sub-total — RCCC</b>	<b>4</b>	<i>Consolidated to 4 engineers covering 20 RCCCs. Exit handover documentation for RCCC configurations begins Year 9.</i>
<b>LCCC — Local Corridor Control Centres (up to 667 corridors)</b>		

Role / Position	FTEs	Application / system support scope and responsibilities
<i>Field technical support for ATMS software agents, edge software installation at each LCCC corridor. Covers ATMS agent health, edge device application configuration, software patches, and planned or corrective on-site technical visits. Most support is delivered remotely; on-site visits are for issues that cannot be resolved remotely.</i>		
LCCC Field Technical Engineers	12	ATMS agent application and edge software support; patch compliance; remote diagnostics; corrective on-site visits for complex faults; exit handover — as-installed configuration documentation per corridor for successor operations team
<b>Sub-total — LCCC</b>	<b>12</b>	<i>All 667 LCCCs live. Mature platform: lower per-site ticket rate, stronger remote resolution capability, improved automation. Coverage ratio: 1 engineer per ~56 LCCCs. Focus shifts to patch compliance and exit handover documentation.</i>
<b>Programme Management &amp; Quality</b> <i>O&amp;M programme governance, quality assurance, patch testing, release coordination, and compliance management across all location tiers.</i>		
O&M Programme Manager	1	O&M delivery; exit management planning (from Year 9); IHMCL interface; final SLA reporting; successor team handover coordination
<b>Sub-total — Programme Management &amp; Quality</b>	<b>1</b>	<i>QA role absorbed by Programme Manager and infrastructure team. Exit management preparation becomes primary focus from Year 9.</i>
<b>GRAND TOTAL — Years 8–10</b>	<b>21</b>	

## 8.5. Work Package 5 — Training, Compliance and Specialised Tools

### 8.5.1. WP-5 Bill of Quantities — Training, Compliance and Specialised Tools/Licenses

BoQ Item	Description	Unit	Qty (Indicative)
WP5-01	ATMS Platform Training Programmes — Design, development, and delivery Includes: Training needs analysis; design and development of training materials (PPT, SOPs, quick-reference cards, video modules); classroom and simulator-based delivery; hands-on exercises on a Training/Sandbox ATMS instance; post-training assessment; training	Per Programme	20

BoQ Item	Description	Unit	Qty (Indicative)
	completion certificates. Each programme accommodates up to 30 trainees. Covers: NCCC Operator Training; RCCC Supervisor Training; LCCC Operator Training; IT/Admin Staff Training; Management Overview Training.		
WP5-02	Cybersecurity VAPT of the ATMS Platform by CERT-In Empanelled Auditor Includes: Engagement and management of a CERT-In empanelled security auditor; VAPT scope definition (Black-box, Grey-box, White-box as agreed); VAPT execution on production/staging environment; full VAPT report with CVSS-scored findings; remediation by the IA; re-test and closure certificate. Platform VAPT to be conducted annually; application-layer VAPT at minimum bi-annually.	Per Assessment	10
WP5-03	Compliance Certification — ISO 27001, STQC, MeitY, NCIIPC assessments Includes: Gap analysis and preparation for each certification; engagement of accredited certification body; documentation support; audit facilitation; certificate issuance and annual surveillance audits. Covers: ISO 27001:2022 (Information Security Management System); STQC IT Security Audit; MeitY Empanelment renewal (if applicable); NCIIPC Critical Information Infrastructure (CII) compliance assessment.	Per Assessment	5
WP5-04	Specialised Engineering and Security Tools — SAST/DAST/API Includes: Annual licence/subscription cost for specialised engineering and security scanning tools used in the ATMS DevSecOps pipeline: Static Application Security Testing (SAST); Dynamic Application Security Testing (DAST); API Security Testing and Monitoring; Software Composition Analysis (SCA) for third-party library vulnerability scanning. Tools to be CERT-In recognised/approved where available.	Per Year	9

## 9. FUNCTIONAL REQUIREMENT SPECIFICATION (FRS)

### 9.1. Overview and Purpose

This Functional Requirement Specification (FRS) defines the mandatory functional and technical requirements for the National ATMS Unified Software Platform, operating as an Integrated Command and Control Centre (NCCC) Platform for all the ATMS projects in India under NHAI. The platform is the central intelligence, command, and coordination layer for the national highway ATMS programme, deployed concurrently across a three-tier hierarchy comprising the National Command & control Centre (NCCC), Regional Command & control Centres (RCCCs), and Local Command & control Centres (LCCCs).

This FRS is structured around the nine software modules mandated by NHAI ATMS Policy 2023 (Chapter 10), and additional other critical modules.

Requirement ID format: FR-[MODULE]-[NNN].

### 9.2. SCOPE BOUNDARY

The ATMS Platform (this specification) is the command, control, coordination, reporting, and analytics layer. It receives structured data from — and sends advisory requests to — the Existing Field Platform Vendor systems that manage TMCS/CCTV/VIDES, ANPR/speed enforcement, VMS,VASD, and e-Challan generation. The ATMS Platform does NOT replicate those field sub-system functions.

Functions WITHIN ATMS Platform Scope	Functions OUTSIDE Scope (Existing Field Platform Vendor)
Data acquisition from AWS, ECBs, 1033 audio, system event logs, health telemetry	CCTV video analytics (VIDES) — AI incident detection from video streams
Incident lifecycle management, SOP orchestration, multi-tier escalation, e-challan generation at RCCC level	ANPR plate recognition, speed enforcement computation, journey time computation (TTMS), violation evidence captures, dispute resolution workflow, Annual calibration and stamping.
GIS dashboard, COP, displaying data received from vendor platforms	VMS content authoring, WYSIWYG composer, and direct VMS device management
Integrated audio communications — 1033, ECB, radio, PTT, VoIP	Deployment of ECB infra and call recording software, EPABX etc., Plotting positioning of ECBs on GIS map
Reporting, analytics, KPI dashboards, national data lake ingestion	Vehicle classification, counting via ATCC software and Cameras
SLA monitoring, asset registry, NMS, maintenance ticketing	Supply of sensors and other infra.
Security, RBAC, audit trail, API gateway to GoI systems and vendor feeds	Red-light / stop-line violation detection (RLVD/SLVD)



All interfaces with the Existing Field Platform Vendor shall be governed by a formal Data Exchange Specification (DES) agreed between IHMCL, the ATMS software development agency (SDA), and the Existing Field Platform Vendor. Standard format: JSON/XML over HTTPS REST or MQTT; authentication: OAuth 2.0 / API key; interface version control maintained in the System Integration Register.

### 9.3. Three-Tier Deployment Architecture

The ATMS NCCC Platform operates as a single, unified software product deployed across three operational tiers. GUI look-and-feel is identical across all tiers; data scope and authority automatically adapt to the authenticated user's tier and jurisdictional assignment.

Tier	Designation	Count	Scope of Visibility
1	<b>National Command &amp; control Centre (NCCC)</b>	1	Entire national highway network — all RCCCs, LCCCs, all field device telemetry
2	<b>Regional Command Centre (RCCC)</b>	20+ Locations	All LCCCs and field assets within the assigned region
3	<b>Local Command Centre (LCCC)</b>	667+ Locations	Field devices on the assigned ATMS project corridor

#### 9.3.1. Common GUI Requirements

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GUI-001</b>	The platform shall provide a unified, browser-based GUI (no proprietary plugins required) that is functionally consistent across NCCC, RCCC, and LCCC tiers. The same application build shall serve all three tiers with tier-adaptive rendering.	Common GUI Framework
<b>FR-GUI-002</b>	The GUI shall automatically scope all data display, search results, maps, dashboards, and reports to the authenticated user's assigned tier and geographic jurisdiction without manual configuration on login.	Auto Data Scoping
<b>FR-GUI-003</b>	The GUI shall support a configurable, widget-based dashboard layout. Operators shall be able to add, remove, resize, and reorder widgets within limits defined by their role. Widget configurations shall be saved per user profile and restored on next login.	Dashboard Customisation
<b>FR-GUI-004</b>	The GUI shall support multiple concurrent monitor configurations: single-screen, dual-screen, triple-screen, and video wall output modes (up to 16	Multi-Monitor & Video Wall Support

Req ID	Requirement Description	Sub-Module / Feature
	simultaneous panels). Display layout shall be saveable as named profiles.	
<b>FR-GUI-005</b>	The GUI shall display a persistent Common Operating Picture (COP) as the primary working view comprising: interactive GIS map, active incident feed with SLA countdown, device health summary bar, and real-time alert ticker. The COP shall not be closeable during an active operator session.	Common Operating Picture
<b>FR-GUI-006</b>	The GUI shall render fully in English and Hindi. The interface language shall be switchable per user session without system restart. All system-generated alerts, notifications, and SOP task descriptions shall be available in both languages.	Bilingual UI
<b>FR-GUI-007</b>	The GUI shall display a persistent, colour-coded tier and jurisdiction indicator (tier name, region/corridor assigned, active session duration) visible at all times on every screen.	Hierarchy Indicator
<b>FR-GUI-008</b>	The GUI shall support dark mode, high-contrast accessibility mode, and configurable font size (normal / large / extra-large) per workstation.	Accessibility Modes
<b>FR-GUI-009</b>	The GUI shall be accessible on standard workstations (minimum 1920×1080 resolution), large-format video wall controllers, and approved tablet devices (minimum 10-inch screen, 1920×1200). Touch-friendly controls shall be available for tablet/touch monitor use.	Device Compatibility
<b>FR-GUI-010</b>	All GUI state changes, operator actions, widget interactions, form submissions, failed actions, and session events shall be logged to the central audit trail with timestamp (UTC + IST), user ID, workstation ID, and session ID. Audit logs shall be immutable.	GUI Audit Logging
<b>FR-GUI-011</b>	The system shall support 'Hot Call' alert functionality. Upon marking an incident on the GIS map, the system shall automatically identify and display nearby Locations of Interest (LOIs) relevant to the incident — hospitals, blood banks, fire stations, police stations, trauma care centres, crane depots, ambulance stations — with contact details and estimated travel time from the incident KP.	Hot Call & LOI Identification
<b>FR-GUI-012</b>	The system shall include a configurable Event Response Mechanism managing event response workflows based on: incident criticality, geographic region, user access level, and automatic or manual execution	Configurable Event Response Mechanism

Req ID	Requirement Description	Sub-Module / Feature
	mode. Both functional dashboards and technical dashboards shall be independently customisable per user role.	
<b>FR-GUI-013</b>	The GUI shall provide contextual help at every screen and data entry point: context-sensitive help text via inline help icon (question mark), sample inputs wherever user data entry is required, field-level validation feedback in real time, and history of recent user inputs for repeat-entry fields.	Contextual Help & Usability
<b>FR-GUI-014</b>	The dashboard shall support multiple input sources for video wall display: PC screen feeds, web application outputs, CCTV stream tokens (from vendor TMCS platform), and other external device feeds. A display layout editor shall allow operators to configure split-screen arrangements.	Multi-Source Video Wall Inputs
<b>FR-GUI-015</b>	The GUI shall display a system-wide health status bar showing: total active incidents, total devices in fault, active weather alerts, WAN connectivity status for all LCCCs, and last data refresh timestamp for each vendor platform feed.	System Health Status Bar
<b>FR-GUI-016</b>	The GUI shall support keyboard shortcuts for all primary operator actions: incident acknowledgement, alarm dismiss, camera PTZ initiation (advisory), VMS advisory request, and SOP task completion. Shortcut mappings shall be configurable by the administrator.	Keyboard Shortcuts
<b>FR-GUI-017</b>	The GUI shall support a 'Quick Action Bar' providing one-click access to: create incident, acknowledge alarm, initiate 1033 call, view corridor status, and generate on-demand report — without navigating away from the current screen.	Quick Action Bar
<b>FR-GUI-018</b>	The platform shall provide a summarized and real-time view of device uptime across all deployed field and system components. It shall also display applicable penalties arising from SLA breaches, including downtime and unattended incidents, in accordance with the defined contractual terms.  The system shall display calculation of uptime/downtime, identification of SLA violations, and tracking of unattended incidents, along with transparent reporting dashboards for monitoring compliance and performance at each tier.	SLA monitoring module

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GUI-019</b>	The platform shall provide a one-click access mechanism to display the relevant Standard Operating Procedures (SOPs) for each incident type across its relevant function. The system shall enable users to view detailed, role-based SOPs mapped to specific incidents, including step-by-step actions, escalation matrices, and responsibilities. Further, the platform shall support automated workflow execution aligned with the defined SOPs, ensuring timely alerts, task assignment, inter-agency coordination, and real-time status tracking for effective incident management.	SOP module.

Note: The features and functionalities specified herein are indicative and represent the minimum requirements for the system. The selected bidder shall ensure that the proposed software platform at each tier is fully scalable, configurable, and customizable to incorporate additional features, functionalities, and enhancements as may be required during the entire project tenure.

Such customization, upgrades, and integration of new features shall be carried out without any additional cost implication to the Authority and shall be treated as part of the scope of work under this contract.

### 9.3.2. NCCC-Specific GUI

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GUI-NCCC-001</b>	The NCCC GUI shall display a national GIS map showing all 20+ RCC regions with real-time aggregate metrics per region: active incident count, traffic count, device availability percentage, alert count, and enforcement revenue (from vendor e-Challan feed). Region tiles shall be colour-coded by operational status.	National Map Overview
<b>FR-GUI-NCCC-002</b>	The NCCC GUI shall provide a national executive dashboard with configurable KPI tiles for MoRTH/NHAI leadership: total incidents (by severity), SLA compliance %, enforcement revenue (YTD), device availability (%), network uptime, and programme KPI actuals vs targets.	Executive Dashboard
<b>FR-GUI-NCCC-003</b>	NCCC operators shall be able to initiate cross-regional incident escalations, send broadcast advisories to multiple RCCCs/LCCCs simultaneously, and view live operational data from any LCCC corridor within the national network.	Cross-Regional Coordination

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GUI-NCCC-004</b>	The NCCC GUI shall provide a programme-level device health heatmap showing real-time availability percentages per region and corridor, drill-down to individual device status, and trend of last 30 days.	Device Health Heatmap
<b>FR-GUI-NCCC-005</b>	The NCCC GUI shall provide MoRTH and NHAI leadership read-only dashboards with programme KPIs, refreshed every 5 minutes. Leadership dashboards shall be accessible via a dedicated URL without navigating the full ATMS interface.	Leadership View

### 9.3.3. RCCC-Specific GUI

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GUI-RCCC-001</b>	The RCCC GUI shall display a regional GIS map covering all LCCC corridors within the assigned region with live incident icons, device health icons, traffic speed overlay (from vendor ATCC/VIDES feed), and weather overlays.	Regional Map View
<b>FR-GUI-RCCC-002</b>	RCCC operators shall be able to remotely assume supervisory view of any LCCC within their region. In emergency conditions and with mandatory authorisation logging, the RCCC operator shall be able to assume full operational control of the LCCC console.	Remote Control LCCC
<b>FR-GUI-RCC-003</b>	The RCCC GUI shall display inter-corridor traffic comparison dashboards comparing: congestion levels, incident frequency, device health, and SLA compliance across all corridors in the region.	Regional Traffic Comparison
<b>FR-GUI-RCC-004</b>	The RCCC GUI shall provide one-click incident escalation to NCCC with mandatory justification capture and automatic pre-population of incident summary, current SOP status, and recommended escalation reason.	Incident Escalation to NCCC

### 9.3.4. LCCC-Specific GUI

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GUI-LCCC-001</b>	The LCCC GUI shall display the assigned corridor in full-detail mode with every field device, camera icon (with status), VMS (with current advisory	Corridor Detail View

Req ID	Requirement Description	Sub-Module / Feature
	state from vendor VMS platform), sensor, and KM-post visible on the GIS map.	
<b>FR-GUI-LCCC-002</b>	The LCCC GUI shall provide a video wall layout mode enabling operators to tile up to 16 simultaneous CCTV stream windows (stream tokens received from vendor TMCS platform) on a multi-monitor workstation, with customisable grid layouts.	Video Wall Tiling
<b>FR-GUI-LCCC-003</b>	The LCCC GUI shall provide an operator console sidebar showing: active incidents (sorted by severity and SLA remaining), pending alarms, VMS advisory request status (from vendor platform), device faults, and SOP task queue.	Operator Console Sidebar
<b>FR-GUI-LCCC-004</b>	The LCCC GUI shall support autonomous operation mode when network connectivity to the RCCC/NCCC is unavailable, preserving all local corridor management functions for a minimum of 168 hours. Upon reconnection, all offline actions and data shall sync automatically.	Autonomous Operation Mode
<b>FR-GUI-LCCC-005</b>	The LCCC GUI shall display a corridor strip chart as an alternative to the GIS map view, showing all KP positions, device locations, active incidents, and current traffic conditions along the linear corridor.	Strip Chart View
<b>FR-GUI-LCCC-006</b>	The LCCC operator console shall display a live PTZ advisory panel showing the status of any pending camera direction advisory submitted to the vendor TMCS platform, and confirmation receipt from the vendor system.	PTZ Advisory Status Panel

#### 9.4. SECTION A — NINE ATMS POLICY-MANDATED MODULES (NHAI ATMS Policy 2023, Chapter10)

<b>01 Data Acquisition Module</b> <b>FR-DAQ</b> <ul style="list-style-type: none"> <li>MQTT v5.0   SNMP   SIP/VoIP</li> <li>AWS, ECB, network devices</li> <li>Vendor VIDES/ANPR/VMS feeds</li> <li>Schema validation &amp; normalisation</li> <li>72-hr LCC buffer   100K events/sec</li> <li>Data lineage &amp; SBOM tracking</li> </ul>	<b>02 Highway Traffic Monitoring &amp; GIS Dashboard</b> <b>FR-HTM</b> <ul style="list-style-type: none"> <li>18-layer GIS Common Operating Picture</li> <li>Traffic speed from vendor ATCC/VIDS</li> <li>18 configurable ITS device layers</li> <li>Emergency vehicle GPS (AIS-140)</li> <li>Historical GIS time-slider replay</li> <li>PM Gati Shakti integration</li> </ul>	<b>03 Incident / Accident Mgmt + ICAD</b> <b>FR-INCD/SOP</b> <ul style="list-style-type: none"> <li>8 detection sources incl. VIDES feed</li> <li>SOP with 5 activity types (incl. nested)</li> <li>Parallel SOP execution across agencies</li> <li>Auto-dispatch via ICAD + NERS 112</li> <li>Incident lifecycle: Detected→PIR</li> <li>Post-Incident Report auto-generated</li> </ul>	<b>04 Integrated Audio Communication</b> <b>FR-AUD</b> <ul style="list-style-type: none"> <li>SIP/VoIP PBX + radio gateway</li> <li>Context-sensitive SOP auto-dial</li> <li>All calls recorded (WORM, 180 days+)</li> <li>Up to 9 concurrent calls</li> <li>In-platform messaging &amp; collaboration</li> <li>PTT/radio integration</li> </ul>	<b>05 Report Generation &amp; Dashboard</b> <b>FR-RPT</b> <ul style="list-style-type: none"> <li>Role dashboards: LCC/RCC/NCC/Leadership</li> <li>Configurable KPI engine (RAG status)</li> <li>Automated daily/weekly/monthly reports</li> <li>Shift handover reports</li> <li>Custom report builder + ad-hoc queries</li> <li>DataLake end-of-day API push</li> </ul>
<b>06 System Administration Module</b> <b>FR-USR/SYS</b> <ul style="list-style-type: none"> <li>MFA mandatory — all users</li> <li>14 RBAC roles + custom roles</li> <li>3 access levels: Read/Write/Modify</li> <li>K8s cloud-native deployment (MEITY GCC)</li> <li>LCC: 72-hr autonomous WAN failover</li> <li>24x7x365   RPO 1hr   RTO 4hr</li> </ul>	<b>07 Communication Module for External Access</b> <b>FR-COM</b> <ul style="list-style-type: none"> <li>National API Gateway (OAuth 2.0/mTLS)</li> <li>PIU/RO read-only portal</li> <li>Police PCR — MPLS/OFC dedicated feed</li> <li>State ICCC bi-directional (DATEX II v3.2)</li> <li>DMC/SDMA — NDMA schema push</li> <li>API health dashboard</li> </ul>	<b>08 API Integrations (VAHAN, FASTag, Rajmarg...)</b> <b>FR-INT</b> <ul style="list-style-type: none"> <li>19 government/agency integrations</li> <li>VAHAN, SARATHI, FASTag/NETC, CCTNS</li> <li>1033 ICAD, Rajmarg, NHAI App, NERS 112</li> <li>eCourts, DigiLocker, IMD, AIS-140</li> <li>PM Gati Shakti, State ICCCs, Police PCR</li> <li>Existing Field Platform Vendor VDIL</li> </ul>	<b>09 Equipment Health Monitoring / NMS</b> <b>FR-NMS</b> <ul style="list-style-type: none"> <li>ATMS-scope devices: AWS/ECB/routers</li> <li>Asset registry — full lifecycle record</li> <li>Auto SLA computation from telemetry</li> <li>Financial penalty auto-calculation</li> <li>Maintenance ticketing (Open→Closed)</li> <li>TSP Contractor Portal — read-only</li> </ul>	

Figure 20: Nine (9) Policy-Mandated Modules

#### 9.4.1. Module 1 — Data Acquisition Module

1. Data acquisition module for acquiring data, video streams and audio streams from field equipment. The Data Acquisition module enables the acquiring of data from the various field equipment in the form of data strings, video streams and audio streams. Examples include:
  - Data strings from VIDES system, ATCC system, WIM system, VAS system;
  - Data strings of date/time and details of events (e.g. the time an Emergency Call was attended to on 1033 or ERT), alarms and faults related to any part of the system;
  - Video Streams from TMCS/CCTV Camera, VIDES Camera;
  - Audio Streams from 1033 Emergency Telephone and Roadside Emergency Telephone;
  - Data strings from ATMS-native AWS, other sensors.
2. The module allows the user to configure acquisition conditions:
  - At regular intervals of time with the interval being user specified (e.g. from the ATCC system);
  - On the occurrence of traffic related events in the field (e.g. from the ATCC system);
  - On demand (e.g. video stream from a CCTV camera);
  - On the occurrence of system related events like equipment failure and restoration, user login/logout.
3. The information thus acquired shall be stored in the ATMS server using an established database package like MySQL or PostgreSQL with preference for enterprise version.
  - INTERFACE: TMCS/CCTV: Receives structured incident detection events (incident type, KP, camera ID, timestamp, confidence score) via vendor API. ATMS does NOT perform video analytics or manage camera streams.



- **INTERFACE: VIDES/ANPR/VSDS/VASD/RADAR/TTMS:** Receives vehicle passage records, plate reads, speed violation flags, and journey time data via vendor API. ATMS does NOT operate ANPR processing or speed detection.
- **INTERFACE: VMS:** Receives VMS device status, current displayed message, and device health state from vendor. ATMS does NOT control VMS content directly.
- **INTERFACE: ECB/MRCS/AUDIO Devices:** Receives audio stream access tokens or snapshot URLs for display in GIS dashboard. call receiving and recording reside with vendor.

#### 9.4.1.1. *Direct Device Data Acquisition*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAQ-001</b>	The system shall ingest real-time data from all managed field devices (TMCS, VIDES, ANPR, AWS, ECBs, UPS units, network equipment, ATMS edge servers etc.) with a maximum ingestion latency of 5 seconds from data origination at the field device.	Direct Device Ingestion
<b>FR-DAQ-002</b>	The system shall support the following ingestion protocols for ATMS-managed devices: MQTT v3.1.1 / v5.0 (IoT sensors, AWS), SNMP v2c / v3 (network devices, UPS), SIP/VoIP (ECB/1033 audio), REST/Webhooks (application events), NTCIP 1201/1202 (field controllers where applicable), and Modbus TCP (legacy field equipment where required).	Multi-Protocol Ingestion
<b>FR-DAQ-003</b>	The system shall implement four configurable acquisition modes for each data source: (a) interval-based with user-specified period (1 second to 24 hours); (b) event-triggered on detection of predefined traffic or system events; (c) on-demand poll initiated by operator or automated rule; (d) system-generated events such as equipment fault, link loss, user login/logout, and configuration change.	Configurable Acquisition Modes
<b>FR-DAQ-004</b>	For AWS sensors, the system shall ingest readings at a configurable interval (default: 5 minutes) for: air temperature, road surface temperature, relative humidity, dew point, wind speed, wind direction (instantaneous and 10-minute average), visibility, precipitation type and intensity, and road surface condition (dry, wet, icy, flooded, chemically wet).	AWS Sensor Ingestion
<b>FR-DAQ-005</b>	The system shall ingest audio streams from all 1033 Highway Helpline calls and all roadside Emergency Call Box (ECB/ERT) activations in real time. Audio streams shall be tagged with ECB ID, KP reference, corridor ID, call start timestamp, and call end timestamp.	Audio Stream Ingestion — 1033 & ECB

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAQ-006</b>	The system shall ingest equipment health telemetry (heartbeat/keepalive) from all registered field devices at intervals not exceeding 60 seconds. A device shall be flagged as 'Communication Lost' if no heartbeat is received within 3 consecutive intervals. The threshold shall be configurable by the administrator.	Equipment Health Telemetry
<b>FR-DAQ-007</b>	The system shall ingest system event logs: user login/logout (with workstation ID), configuration changes (with before/after values), software restarts, storage threshold warnings, and security events. All system event logs shall be forwarded to the SIEM in real time.	System Event Log Ingestion
<b>FR-DAQ-008</b>	The system shall perform automated real-time data quality validation on all ingested data: range checks (physical plausibility), rate-of-change checks (spike detection), completeness checks (mandatory fields), and cross-source consistency checks. Invalid data shall be flagged, quarantined, and not used in operational dashboards without analyst review.	Data Quality Validation
<b>FR-DAQ-009</b>	The system shall provide data buffering at each LCC: a minimum of 72 hours of all acquired data shall be buffered locally for autonomous operation during WAN outage. Buffered data shall be automatically synchronised to the national data lake upon WAN restoration in chronological order.	Local Data Buffering
<b>FR-DAQ-010</b>	The system shall compress all ingested data before storage using lossless compression (minimum LZ4 or equivalent). Compression ratio and storage utilisation shall be reported on the system administration dashboard.	Data Compression

#### 9.4.1.2. Vendor Platform Data Ingestion

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAQ-011</b>	The system shall receive structured incident detection events from the Existing Field Platform Vendor's VIDES system within 5 seconds of the detection event. Each event shall contain at minimum: incident type, camera ID, KP reference, corridor ID, detection timestamp, confidence score, and thumbnail image URL.	VIDES Event Ingestion

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAQ-012</b>	The system shall receive vehicle passage records and speed violation flags from the Existing Field Platform Vendor's ANPR/VSDS system. Each vehicle passage record shall contain: plate number (or masked equivalent), vehicle class, camera ID, KP, direction, lane, timestamp, speed (where available), and a unique passage reference ID.	ANPR/VSDS Data Ingestion
<b>FR-DAQ-013</b>	The system shall receive journey time and average speed data from the vendor ANPR/TTMS platform for configured ANPR pairs at intervals not exceeding 60 seconds.	Journey Time Feed Ingestion
<b>FR-DAQ-014</b>	The system shall receive VMS device status updates from the vendor VMS platform at intervals not exceeding 60 seconds. Status data shall include: device ID, current displayed message content (text), device health status (online/offline/degraded/fault), last command acknowledgement timestamp.	VMS Status Ingestion
<b>FR-DAQ-015</b>	The system shall receive e-challan lifecycle status updates from the vendor enforcement platform (generated, notified, paid, disputed, defaulted, court-escalated, settled) via webhook or polling interval not exceeding 5 minutes.	e-Challan Status Feed
<b>FR-DAQ-016</b>	The system shall receive structured device health telemetry from the Existing Field Platform Vendor's NMS for VIDES cameras, ANPR cameras, VMS units, and speed radars, at intervals not exceeding 5 minutes. This telemetry shall feed the ATMS SLA computation engine.	Vendor NMS Health Telemetry
<b>FR-DAQ-017</b>	The system shall maintain a data feed health monitor for each vendor API endpoint: tracking last successful receive timestamp, message volume per hour, error rate, and schema validation failure rate. Alerts shall be raised if any feed is silent for more than 2× the expected interval.	Vendor Feed Health Monitoring
<b>FR-DAQ-018</b>	All ingested vendor data shall be schema-validated against the Data Exchange Specification (DES) before storage. Schema versions shall be tracked. Any schema mismatch shall be alerted to the System Administrator and logged for vendor notification.	Schema Validation & Versioning

#### 9.4.1.3. Data Pipeline and Storage

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAQ-019</b>	The system shall implement a data normalisation layer converting heterogeneous data formats from field devices and vendor platforms into a common canonical data schema (CDS) before storage. The CDS shall be documented and published as part of the System Integration Register.	Data Normalisation
<b>FR-DAQ-020</b>	The event processing pipeline shall handle a sustained throughput of minimum 100,000 events per second at NCCC tier with automatic horizontal scaling using Kubernetes-based container orchestration. Sustained ingestion performance shall be demonstrated during FAT.	Event Throughput & Scalability
<b>FR-DAQ-021</b>	All ingested data shall be stored in the ATMS national data lake on MEITY-empanelled cloud infrastructure with geo-redundant replication across DR availability zones. No personal data of Indian citizens shall be stored outside India.	National Data Lake & Localisation
<b>FR-DAQ-022</b>	The system shall provide a drag-and-drop visual integration studio enabling administrators to define data transformation, filtering, routing, and enrichment pipelines without programming. Pipelines shall be version-controlled, auditable, and testable against sample payloads in a staging environment.	No-Code Pipeline Builder
<b>FR-DAQ-023</b>	The system shall maintain data lineage records for every data object: source system, ingestion timestamp, schema version, all transformation steps applied, and consuming applications/modules. Lineage shall be queryable via the ad-hoc query builder.	Data Lineage
<b>FR-DAQ-024</b>	The system shall provide built-in data transformation functions: JSON to XML, CSV to JSON, date/time normalisation (UTC conversion), unit conversion (metric/imperial), string normalisation, and coordinate system transformation (WGS84/UTM). Custom transformation functions shall be configurable by authorised Data Analysts.	Data Transformation Functions
<b>FR-DAQ-025</b>	The system shall be ODBC-compliant and capable of interfacing with standard RDBMS platforms (PostgreSQL, MySQL Server) ensuring data accessibility to standard reporting and analysis tools without proprietary drivers.	ODBC Compliance

#### 9.4.2. Module 2 — Highway Traffic Monitoring Module & GIS Dashboard

1. This module shall support effective Traffic monitoring on the highway. The targeted road section or the entire stretch shall be depicted on the Large display (video wall) and ITM workstation in the form of animated screens including Graphic User interfaces not limited to specified under Clause 816.1 to 816.17 of Specifications for Road and Bridge Works of MoRTH.
2. An interactive GIS map (free and open source such as Open Street Maps etc. or proprietary) shall be available for all workstations and on the video wall. The GIS map should include:
  - Icons for CCTV, VIDS, VMS and other devices.
  - On clicking the device it should open up the video feed of the cameras or show the message being displayed on the VMS and allowing for modifying the messages from there if user has permission. It should be possible to update the message on the VMS from here.
  - Any incident triggered from VIDES or TMCS shall appropriately modify the icon of the camera on the GIS map to call attention of operators.
  - When the video stream for VIDES or TMCS is clicked and pulled up, it should be possible to “create an event” for the dispatch. This would automatically capture the photo from the stream, location and allow to choose type of incident detected if manual. This event in one-click should be possible to be dispatched to nearby emergency vehicle if ICAD has been setup.
  - The map should show at all times the live location of the Crane, Ambulance and RPVs through data received from AIS140 or ICAD.
  - Section of the highway stretch should highlight to show traffic flow as identified by VIDS (different colours for different flows, separated by direction).
  - If any device is not functioning, the same shall also be easily seen from this GIS map if the icon of the device is appropriately changed during malfunction.
  - The GIS map shall show if any event has been passed to ATMS through 1033, iCAD or Rajmarg Yatra based on the location of the incident. It should be automated based on rules and thresholds.
  - It should be possible to click on an incident either from VIDS, TMCS, ICAD, 1033 or Rajmarg or Manually on Any location of the Map and create an event for emergency response dispatch.
  - The GIS map shall have an equivalent strip chart interface.
  - The map shall allow zooming into relevant sections with no loss to definition.
  - The details of the project-specific composition of the GUI will be finalized during the project execution phase between the Service Provider and NHAI/IHMCL (or its authorized representative).

#### **9.4.2.1. Map Platform and Navigation**

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-HTM-001</b>	The system shall provide a national GIS map platform displaying the complete NHAI highway network with: full route alignments, KP reference markers, road attributes (number of lanes, carriageway type, median type, speed limit, lane configuration), toll plazas, and administrative boundaries (state, district). Map shall be integrated with PM Gati Shakti to <b>integrate and coordinate infrastructure development across multiple sectors</b> such as roads, railways, ports, airports, and logistics.	National Map Base Layer
<b>FR-HTM-002</b>	The GIS map shall support seamless zoom from a national overview (full NH network visible at sub-5m screen scale) to street-level resolution (sub-50m). All device icons, incident markers, and data overlays shall auto-scale and remain legible at all zoom levels.	Zoom Range
<b>FR-HTM-003</b>	Standard map navigation shall include: pan, zoom in/out, zoom to extent, zoom to selected device/incident, previous/next zoom history, and search by corridor name, road number, KP reference, toll plaza name, or place name via Geo-coding API.	Navigation & Search
<b>FR-HTM-004</b>	The system shall support multiple base map tile providers selectable per session: OpenStreetMap (default), Google Maps, Bing Maps, and ESRI ArcGIS or equivalent. An offline cached base map shall be maintained for all LCCC corridors for use during internet connectivity loss, updated automatically on a weekly schedule.	Multi-Provider Base Map
<b>FR-HTM-005</b>	The GIS map shall include an equivalent strip chart interface showing all KP positions, field device locations, active incidents, and traffic conditions along the linear corridor. The strip chart shall be synchronised with the GIS map so that selecting an item on one, updates the other.	Strip Chart Interface

#### 9.4.2.2. *Device and Situational Awareness Layers*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-HTM-006</b>	The GIS map shall support configurable, independently-toggleable ITS device layers: CCTV/TMCS, ANPR/VIDS/VASD, RADAR, VMS, ATCC, Radar, Weather Stations (AWS), MRCS/ECBs/ERTs, RLVD devices, SLVD devices, and Weigh-in-Motion (WIM) stations. Device icons shall reflect	Configurable ITS Device Layers

Req ID	Requirement Description	Sub-Module / Feature
	health status received from ATMS NMS or vendor platform feeds (green/amber/red/grey-offline).	
<b>FR-HTM-007</b>	Clicking any device icon on the GIS map shall open a contextual device panel displaying: device ID, type, manufacturer, KP, last communication timestamp, current operational status, and — for cameras — a thumbnail or stream token received from the vendor TMCS platform. For VMS, the current displayed message (from vendor VMS platform) shall be shown.	Device Detail Click Panel
<b>FR-HTM-008</b>	The system shall display real-time traffic speed conditions on all highway segments using a colour-coded speed band overlay: green (free-flow, >80% posted limit), yellow (moderate, 60–80%), orange (heavy congestion, 40–60%), red (near-standstill, <40%). Data sourced from vendor ATCC/VIDS platform, updated at intervals not exceeding 60 seconds. Speed limits for every KP reference section is defined in rules engine for the corridor in LCCC software.	Traffic Speed Colour Layer
<b>FR-HTM-009</b>	All active incidents and road condition shall be displayed on the GIS map with severity-coded icons (green/yellow/orange/red) positioned at their exact KP location, updating in real time as incident status changes. Hovering over an incident icon shall display a tooltip with: incident ID, type, severity, time elapsed, and current SLA status.	Live Incident Layer
<b>FR-HTM-010</b>	The GIS map shall display real-time weather conditions at each AWS location using overlay icons for: rain (with intensity), fog (with visibility value), ice, wind (with speed and direction), and flood warning. AWS icons shall change colour when any threshold is breached.	Weather Overlay Layer
<b>FR-HTM-011</b>	Enforcement events in progress (from vendor e-Challan feed) shall be displayed on the GIS map as distinct icons, enabling supervisors to monitor enforcement activity distribution across the corridor.	Enforcement Activity Layer
<b>FR-HTM-012</b>	The GIS map shall display camera Field of View (FOV) cones for a selected camera or all cameras simultaneously (toggled layer), to assist corridor coverage gap analysis. FOV data shall be stored in the device registry and updatable by administrators.	Camera FOV Overlay
<b>FR-HTM-013</b>	The map shall display at all times the live GPS location of all Route Patrol Vehicles (RPVs), Ambulances, Cranes, and Emergency Response Teams (ERTs) through data received from AIS-140 transponders or the ICAD	Emergency Vehicle Live Tracking



Req ID	Requirement Description	Sub-Module / Feature
	integration. Vehicle icons shall show vehicle ID, operator name, and last update timestamp on hover.	
<b>FR-HTM-014</b>	The GIS map shall show all events passed to ATMS through 1033 iCAD, Rajmarg Yatra, and NHAI Mobile App, positioned at their geo-tagged locations. These crowd-sourced events shall be distinguished from sensor/automated events by a distinct icon style.	Crowd-Sourced Event Layer

#### 9.4.2.3. Incident and Geofencing Map Tools

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-HTM-015</b>	Operators shall be able to create an incident directly from the GIS map by right-clicking or long-pressing a location, which pre-populates the incident creation form with: KP reference, corridor ID, nearest registered camera ID, and nearest AWS weather station data.	Map-Click Incident Creation
<b>FR-HTM-016</b>	Operators shall be able to draw polygons, polylines, and point markers on the GIS map and associate them with incident records for multi-location incidents (e.g. long-distance debris, multi-vehicle pile-up spanning multiple KPs).	Incident Map Annotation
<b>FR-HTM-017</b>	Administrators shall be able to define geofenced zones of arbitrary shape on the GIS map. Entry or exit of a watch-listed or flagged vehicle (watch-list data from vendor ANPR platform) into a geofenced zone shall generate an automated alert to the LCCC operator within 30 seconds of the ANPR read.	Geofencing & Watch-List Alerts
<b>FR-HTM-018</b>	The GIS map shall support display of heat maps for: incident frequency, violation frequency (from vendor e-Challan feed), Road condition and traffic congestion. Heat maps shall be computable over user-defined time ranges from 1 hour to 5 years.	Heat Map Display
<b>FR-HTM-019</b>	The system shall calculate and display the shortest route between any two GIS map locations, considering highway directionality, and indicate estimated travel time based on current traffic speed data received from the vendor ATCC/VIDS platform.	Route Analysis

**9.4.2.4. Historical Replay and GIS Data Management**

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-HTM-020</b>	The system shall provide a GIS time-slider feature enabling operators to replay historical traffic conditions, incident positions, device states, and weather conditions for any date and time within the data retention window. Playback speed shall be selectable: 1×, 5×, 10×, 60× real-time.	Historical GIS Replay
<b>FR-HTM-021</b>	Operators shall be able to save named GIS map views (layer configuration + zoom level + map centre + time-slider position) and recall them instantly from a favourites list. Named views shall be shareable between operators within the same tier.	Saved Map Views
<b>FR-HTM-022</b>	Operators shall be able to capture a snapshot of the current GIS map view (all visible layers, current zoom and centre) and attach it to an incident record, SOP task, or export as a geo-referenced PNG image.	Map Snapshot Export
<b>FR-HTM-023</b>	The system shall support GIS data export in GeoJSON, Shapefile, KML, and CSV formats for integration with external GIS platforms (e.g., ESRI ArcGIS, QGIS, PM Gati Shakti).	GIS Data Export Formats
<b>FR-HTM-024</b>	The GIS database shall include detailed POI categories: Health Services (hospitals, blood banks, medical centres, trauma care), Community Services (fire stations, police stations, ATMs, banks, government buildings), Transportation Facilities (bus terminals, railway stations, petrol pumps, metro stations, airports), and Road Amenities (flyovers, underpasses, rest areas, emergency lay-bys). POI data shall be kept current through scheduled automated updates and authorised manual edits.	GIS POI Database
<b>FR-HTM-025</b>	The GIS database shall include comprehensive road network data: city arterial roads, urban streets, national highways, state highways with road name, classification, lane count, speed limits, and directionality. Administrative boundaries shall include state, district, sub-district, and town boundaries.	Road Network & Admin Data
<b>FR-HTM-026</b>	The system shall integrate with the PM Gati Shakti GIS platform, sharing real-time traffic conditions, incident events, and ATMS asset data in the	PM Gati Shakti Integration

Req ID	Requirement Description	Sub-Module / Feature
	PM Gati Shakti standard data format for national-level infrastructure planning and coordination.	

#### 9.4.3. Module 3 — Incident / Accident Management Module with Integrated Computer Aided Dispatch (ICAD)

This module shall support Incident / Accident Management by:

1. Allowing the Traffic Management console operator to locate and mark (with a mouse) an accident / incident on the GIS map of the highway and initiate the Incident management actions;

Displaying a contextual on-line checklist for the operator to follow in sequence; Further the clicking on each item of the checklist shall automatically activate the related ATMS equipment to aid in the management viz.

- Seamless audio connection for the Traffic Management console operator, via the integrated audio communication unit, irrespective of the communication media (Mobile radio, Mobile phone/landline, road-side Emergency telephone), to the ambulance, Trauma Care Centres, Patrol & other O&M vehicles.
- Automatic Pan, Tilt and Zoom of the nearby camera to view the accident
- Bringing on the VMS message edit screen (by interfacing with the VMS Control software to create and dispatch messages to VMS boards and mobile apps of registered road users). The checklist itself shall be derived from the relevant Traffic Management and rescue procedures captured either in the Operation (O&M) manual of the highway or based on world-class best practices.
- Logging the time-stamp of the operator operating each element of the checklist to aid in 'post-facto' analysis of the operator's performance towards establishing his /her efficiency and further training needs and SLA monitoring needs.
- Automatically performing pre-defined actions related to each of the above elements (e.g. Identification of the accident spot on the road shall control the nearby CCTV cameras to 'look' in the direction of the accident spot)
- Aiding on-line tracking (via GPS) of the various O&M vehicles like the Ambulance, Tow-vehicle and the Patrol vehicle supported with dynamic display of information like shortest route, travel time to the accident spot, Trauma Care Centre etc.
- Providing a user-programmable facility, as an aid, for the automatic generation of VMS messages depending on incidents based on e.g. information measured by the MET/AWS sensors and sensors installed on the highway (e.g. the generation of a Visibility Alert signal in the event of visibility going below 1 km). This module shall alert the operator on generating the message which shall then be deployed on the operator's approval.

- The detailed workflow of this module involving various checklists, shall be finalized between the service provider and NHAI during the project execution phase.
- The module should be able to have complete functionalities as given under Chapter -4 (ATMS Policy 2023) including incidence response and facilitating generation of e- challan through NIC.

#### 9.4.3.1. Incident Detection and Source Integration

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INCD-001</b>	The system shall accept incident detection inputs from the following sources: (a) VIDES structured event feed from Existing Field Platform Vendor (automated AI detection); (b) ANPR/VSDS/VASD/RADAR feed — journey-time outliers and speed violations flagged by vendor; (c) ECB/1033 calls received directly by ATMS audio module; (d) Rajmarg Yatra crowd reports (with location, photo, incident type); (e) NHAI Mobile App reports; (f) iCAD dispatch system notifications; (g) Manual creation by operators from GIS map or patrol report; (h) Social media intelligence alerts from the multi-source fusion module.	Multi-Source Detection
<b>FR-INCD-002</b>	The system shall create a candidate incident record within 5 seconds of receiving a detection event from any source. Each candidate shall include: source identifier, raw detection data, originating system, detection timestamp (UTC + IST), and geo-location (KP + GPS coordinates).	Candidate Incident Creation
<b>FR-INCD-003</b>	The system shall automatically deduplicate candidate incidents: any two detection events from different sources within a 500-metre radius and within a 5-minute window shall be evaluated for merge. The system shall present the deduplication candidate to the operator for confirmation, with supporting evidence from each source.	Incident Deduplication
<b>FR-INCD-004</b>	For incidents detected via VIDES, the system shall display the detection event details (bounding box overlay reference, event type, confidence score, camera ID, KP reference) in the operator confirmation panel. The operator shall confirm or reject the AI-detected event with one click. Rejected events shall be logged with rejection reason for vendor model improvement feedback.	VIDES Detection Confirmation

**9.4.3.2. Incident Record and Classification**

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INCD-005</b>	The system shall create a unique incident record for every confirmed incident containing mandatory fields: incident ID (system-generated, unique globally), date/time of detection, date/time of confirmation, KP location (start and end for extent-based incidents), GPS coordinates, corridor ID, incident type, incident sub-type, incident severity, detection source, assigned LCCC operator, assigned RCC supervisor, and current lifecycle status.	Incident Record Structure
<b>FR-INCD-006</b>	The system shall classify each incident by type from the following taxonomy: Accident (Fatal / Injury / Property Damage Only), Breakdown, Debris on Road, Wrong-Way Driving, Stopped Vehicle (lane obstruction), Pedestrian on Carriageway, Fire, Flooding, Overloading, Road Works (Planned / Unplanned), Weather Hazard, Animal on Road, Medical Emergency, and Other (with mandatory free-text description).	Incident Type Taxonomy
<b>FR-INCD-007</b>	The system shall classify each incident by severity: Minor (no lane obstruction; clearance < 30 minutes expected), Moderate (partial lane obstruction), Major (full carriageway obstruction; multi-vehicle or injury), and Catastrophic (multi-fatality, infrastructure damage, or road closure > 4 hours).	Severity Classification
<b>FR-INCD-008</b>	Operators shall be able to manually create incidents using a structured form pre-populated from GIS map coordinates. Mandatory fields shall include: type, sub-type, severity, location (KP or GPS), detection source, and initial description. Optional fields: vehicle registration (from ANPR data if available), number of vehicles involved, estimated casualties, and road obstruction extent.	Manual Incident Creation
<b>FR-INCD-009</b>	The system shall allow the operator to link one or more CCTV stream tokens (received from vendor TMCS platform), ANPR vehicle passage records, weather readings, and VMS advisory request records to an incident record at any point in the lifecycle.	Evidence Linking to Incident
<b>FR-INCD-010</b>	The system shall compute and display an estimated incident clearance time for each confirmed incident based on: incident type, severity, historical clearance data for similar incidents on the same corridor type, current time of day, and current weather conditions.	Estimated Clearance Time

**9.4.3.3. Notification and Escalation**

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INCD-011</b>	Upon incident creation, the system shall notify the assigned LCCC operator via: on-screen alert pop-up (with audio alarm tone configurable per incident severity), SMS to operator's registered mobile, and display of incident in the 'Active Incidents' sidebar sorted by severity and SLA countdown.	LCCC Operator Notification
<b>FR-INCD-012</b>	Moderate and above severity incidents shall be automatically notified to the parent RCCC within 60 seconds of confirmation via: on-screen alert on the RCCC console, SMS/push notification to the RCCC supervisor, and display on the RCCC regional GIS map with severity icon.	RCCC Escalation Notification
<b>FR-INCD-013</b>	Major and Catastrophic incidents shall be automatically notified to NCCC within 60 seconds of confirmation via: NCCC dashboard alert, NCCC leadership dashboard auto-refresh, SMS to designated NCCC supervisor, and national GIS map icon update.	NCCC Escalation Notification
<b>FR-INCD-014</b>	The system shall track configurable SLA response timers per severity level: (a) Acknowledgement SLA — time from detection to operator acknowledgement; (b) Dispatch SLA — time from confirmation to first resource dispatch; (c) Clearance SLA — time from confirmation to incident cleared status. All three timers shall be displayed live in the operator console and on the incident record.	SLA Timer Tracking
<b>FR-INCD-015</b>	If an incident is not acknowledged within the SLA acknowledgement period, the system shall automatically escalate it to the next tier supervisor (LCCC→RCCC→NCCC) with an escalation alert and mandatory documentation of reason for non-acknowledgement by the escalating tier as per pre-defined and configurable SOP.	SLA Breach Auto-Escalation
<b>FR-INCD-016</b>	The system shall integrate with NHAI 1033, NERS 112 to automatically forward Major and Catastrophic incident notifications within 2 minutes of Catastrophic classification, including: GPS coordinates, incident type, severity, estimated number of casualties, and current weather at incident location.	NERS 112 Auto-Notify
<b>FR-INCD-017</b>	The system shall provide an RCCC one-click escalation to NCCC with auto-populated escalation summary (incident ID, type, severity, time elapsed, SOP status, resources deployed) and mandatory free-text justification field. Escalation action shall be logged with escalating operator ID and timestamp.	Manual Escalation to NCCC

**9.4.3.4. SOP Workflow and Response Orchestration**

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SOP-001</b>	The system shall automatically assign the relevant Standard Operating Procedure (SOP) to an incident record based on incident type, sub-type, and severity at the time of incident confirmation. Multiple SOPs may be assigned concurrently for complex incidents.	Auto-SOP Assignment
<b>FR-SOP-002</b>	Each SOP shall comprise an ordered task list. Each task shall contain: unique task ID, task description (in English and Hindi), responsible role, target completion time from incident start, action type, preconditions (if any), and completion checkbox with mandatory completion note.	SOP Task Structure
<b>FR-SOP-003</b>	The system shall support five SOP activity types: (a) Manual Activity — performed by assigned operator with description and completion status; (b) Automation Activity — triggers a predefined automated system action (e.g., camera advisory to vendor, VMS advisory request); (c) If-Then-Else — conditional branching based on real-time data criteria; (d) Notification Activity — generates and dispatches a configurable communication (email/SMS/PTT) to configured recipients; (e) Nested SOP Activity — triggers execution of another predefined SOP as a child workflow.	Five SOP Activity Types
<b>FR-SOP-004</b>	The SOP system shall support parallel execution of multiple tasks without serialisation constraints. Tasks assigned to different agencies or operators shall be tracked concurrently. The SOP Gantt view shall display all tasks on a timeline with actual vs. target completion status.	Parallel SOP Execution
<b>FR-SOP-005</b>	The system shall support an approval workflow: an SOP or specific SOP step requiring approval shall not proceed until an authorised senior operator or supervisor approves it via the ATMS interface. Approval shall be achievable from mobile devices. All approval/rejection decisions shall be logged with timestamp, user ID, and mandatory written justification.	SOP Approval Workflow
<b>FR-SOP-006</b>	The SOP authoring tool shall allow authorised administrators to create, edit, version-control (with change history), and deactivate SOPs without requiring technical skills. SOPs shall support English and Hindi task	SOP Authoring & Version Control



Req ID	Requirement Description	Sub-Module / Feature
	descriptions. A SOP test/simulation mode shall allow SOPs to be validated against simulated incident data before activation.	
<b>FR-SOP-007</b>	Completed SOP tasks shall be timestamped and attributed to the operator who marked them complete, creating a full action audit trail within the incident record. Incomplete tasks shall require a mandatory justification note before incident closure is permitted.	SOP Task Audit Trail
<b>FR-SOP-008</b>	The system shall permit simultaneous multi-agency collaboration on a single incident SOP: LCCC, RCCC, police, ambulance, NHAI patrol, and highway maintenance units shall each see and update their assigned SOP tasks concurrently. Changes by one agency shall be visible to all others in real time.	Multi-Agency SOP Collaboration
<b>FR-SOP-009</b>	Incident-triggered automated actions shall include, at minimum: (a) dispatch PTZ advisory request to vendor TMCS platform (pan nearest camera to incident KP); (b) dispatch VMS advisory message request to vendor VMS system for upstream signs; (c) emergency vehicle dispatch request to iCAD system; (d) NERS 112 notification for qualifying incidents; (e) weather condition capture from nearest AWS at time of incident detection.	Automated Incident Actions
<b>FR-SOP-010</b>	The system shall support outbound SOP adapters that can be configured as executable tasks within a SOP to trigger actions, transmit data, or invoke third-party devices and applications, including invocation of external REST APIs as part of SOP step execution.	SOP Outbound Adapters & API Tasks
<b>FR-SOP-011</b>	Authorised users shall be able to stop or abort an SOP prior to completion, subject to RBAC controls, with mandatory documentation of reason. Authorised users shall also be able to add free-text comments to any in-progress SOP task at any time. Both actions shall be logged in the audit trail.	SOP Stop / Comment

#### 9.4.3.5. Incident Lifecycle, Closure and Analytics

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INCD-018</b>	Each incident shall progress through a defined, locked lifecycle: Detected → Confirmed → Response Dispatched → Under Resolution → Cleared →	Incident Lifecycle States

Req ID	Requirement Description	Sub-Module / Feature
	Closed → Post-Incident Review (PIR). Backwards state transitions shall require supervisor authorisation and mandatory reason.	
<b>FR-INCD-019</b>	Incident closure shall require: (a) completion of all mandatory SOP tasks or documented justification for each incomplete task; (b) operator confirmation that the highway is clear or restricted condition is documented; (c) supervisor approval for Major and Catastrophic incidents. System shall block closure if mandatory fields are empty.	Mandatory Closure Requirements
<b>FR-INCD-020</b>	The system shall automatically generate a post-incident report (PIR) upon closure, containing: full event timeline (detection to closure), all SOP tasks with operator attribution, resources deployed (vehicles dispatched from iCAD), VMS advisory requests made and their status, ANPR data (vehicle counts at incident KP, from vendor), SLA performance summary, weather at time of incident, and root cause (operator-entered). PIR shall be auto-distributed to configured supervisors.	Post-Incident Report
<b>FR-INCD-021</b>	The system shall provide an incident replay viewer enabling supervisors to replay the full sequence of operator actions, GIS state changes, SOP task completions, and communications log for any closed incident. Replay shall be playable at variable speed.	Incident Viewer Replay
<b>FR-INCD-022</b>	All incident records shall be archived in the national data lake with a minimum retention period of 1 year. Incident records shall be searchable by type, severity, corridor, date range, operator, and SLA outcome.	Incident Data Retention
<b>FR-INCD-023</b>	The system shall provide incident hotspot analysis dashboards identifying: road segments with disproportionately high incident frequency, times of day and days of week with elevated risk, weather conditions correlated with incident occurrence, and recurring incident types per corridor. Hotspot analysis shall be exportable as GIS layers.	Incident Hotspot Analysis
<b>FR-INCD-024</b>	The system shall provide comparative incident trend reports: year-on-year, month-on-month, and corridor-vs-corridor. Reports shall show: incident count by type and severity, average response times, SLA compliance rates, and mean clearance time by incident type. Exportable in PDF and Excel.	Incident Trend Reports
<b>FR-INCD-025</b>	The system shall provide an Incident Learning Module: upon PIR completion, the system shall flag recurring incident patterns (same KP, same type, >3 occurrences in 30 days) and propose preventive action	Incident Learning Module

Req ID	Requirement Description	Sub-Module / Feature
	recommendations to the LCCC/RCCC supervisor, drawing from the historical incident database.	

#### 9.4.4. Module 4 — Integrated Audio Communication Module

This module shall interface with and control the integrated audio communication unit to aid the operator seamlessly communicate with various stakeholders via a host of communication media like telephone landlines, mobile telephony, mobile wireless etc.

The Integrated Audio communication unit enables the Traffic Manager/operator to communicate with all stakeholders in a seamless manner irrespective of the medium of communications using a hardware like a digital telephone exchange that supports software control. This unit allows the Traffic manager wearing a headset with microphone (or a handset) to seamlessly communicate with the stakeholders using various audio communication media like Mobile wireless radios, Mobile (GSM) telephones, Telephone landlines, Mobile radio communication system (MRCS) and the road-side Emergency Telephone. Communication is initiated on selection of a context sensitive checklist element or by selection of suitable icons on the ITM workstation screen or GIS MAP. This unit shall support communication between the Traffic manager and a single stakeholder or a group of stakeholders. All calls shall be logged and recordings kept for a period of 30 days or until SLAs have been assessed, whichever is larger.

##### 9.4.4.1. Unified Communication Interface

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-AUD-001</b>	The system shall provide an Integrated Audio Communication capability enabling the operator to communicate with all stakeholders — ambulance services, trauma care centres, police PCR, highway patrol (RPV audio and video streams), crane operators, highway maintenance, NHAIT RO/PIU officials, and civil agencies — across all communication media from a single operator workstation without switching applications.	Unified Communication Interface
<b>FR-AUD-002</b>	The communication system shall support the following media types simultaneously from the same operator station: (a) Mobile radio (UHF/VHF); (b) GSM/mobile telephone; (c) PSTN landline; (d) VoIP/SIP; (e) Roadside Emergency Telephone (ECB/ERT via dedicated 1033 helpline); (f) Internal ATMS intercom between operator workstations at NCCC/RCCC/LCCC.	Multi-Media Communication

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-AUD-003</b>	Communication shall be initiated via: (a) context-sensitive SOP checklist item click (which auto-identifies and dials the assigned stakeholder); (b) selection of icons on the ITM workstation screen; (c) manual dialing from the operator communication panel; (d) incoming call acceptance from any connected communication medium.	Communication Initiation Methods
<b>FR-AUD-004</b>	The system shall support group/conference calls to multiple stakeholders simultaneously. The operator shall be able to add or remove parties from a live conference call. A visual participant panel shall show all active parties in the conference.	Group / Conference Calls
<b>FR-AUD-005</b>	The call management system shall support holding up to 9 simultaneous calls in queue. Calls shall be prioritised by incident severity. The system shall allow call transfer, call-back to any ECB, and patching of ECB calls to an external telephone, mobile radio, or local intercom.	Call Queue & Management
<b>FR-AUD-006</b>	Disconnection of a call shall be permitted only after the call is answered; the system shall prevent accidental disconnection of emergency calls. An on-screen confirmation prompt shall be displayed before ending any active call linked to a Catastrophic incident.	Disconnection Control

#### 9.4.4.2. *Call Recording and Audit*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-AUD-007</b>	All calls — inbound from 1033, NERS, ECB, and outbound to agencies — shall be automatically recorded in full audio from call initiation to termination. Recordings shall be indexed with: ECB ID or caller number, KP reference, corridor, call start/end timestamp (UTC + IST), operator ID, workstation ID, and linked incident ID (if applicable).	Automatic Call Recording
<b>FR-AUD-008</b>	All call recordings shall be retained for a minimum of 30 days or the full O&M SLA assessment period (whichever is greater). Recordings linked to incidents shall be retained for the lifetime of the incident record (minimum 1 year). Recordings shall be stored in the national data lake with the same encryption standards as operational data.	Call Recording Retention
<b>FR-AUD-009</b>	Call recordings shall be tamper-proof: digitally signed at the time of capture with a hash. Any post-capture modification shall invalidate the signature and generate a security alert. Recordings shall not be deletable	Recording Tamper-Proofing

Req ID	Requirement Description	Sub-Module / Feature
	by any user including system administrators without formal NHAI approval and dual-authority confirmation.	
<b>FR-AUD-010</b>	The call log shall be searchable by: operator ID, ECB ID, date/time range, corridor, incident ID, call duration, and media type. Search results shall display a waveform preview and one-click playback.	Call Log Search & Playback
<b>FR-AUD-011</b>	The system shall generate automated call statistics reports: total call volume per operator per shift, average call handling time, unanswered call rate, call type distribution (ECB vs. outbound agency), and calls-per-incident. Reports shall be available at LCCC, RCCC, and NCCC levels.	Call Statistics Reports
<b>FR-AUD-012</b>	The system shall perform real-time call quality monitoring: packet loss, jitter, and MOS score for VoIP connections. Quality alerts shall be raised if call quality falls below configured thresholds. Historical call quality data shall be available for SLA assessment.	Call Quality Monitoring

#### 9.4.4.3. *In-Platform Messaging and Collaboration*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-AUD-013</b>	The system shall provide an in-platform text messaging module enabling real-time communication between operators across NCCC, RCCC, and LCCC tiers. Message history shall be retained for a minimum of 1 year and shall be searchable by sender, recipient, corridor, and keyword.	In-Platform Messaging
<b>FR-AUD-014</b>	The system shall automatically create an incident-scoped collaboration thread for each Major or Catastrophic incident. The thread shall be accessible to all agencies assigned to the incident (LCCC, RCCC, NCCC, police, ambulance, NHAI patrol). GIS map snapshots, CCTV stream tokens, and document attachments shall be shareable within threads.	Incident Collaboration Threads
<b>FR-AUD-015</b>	NCCC/RCCC supervisors shall be able to push broadcast advisory messages simultaneously to all LCCC operators within their jurisdiction. Broadcasts shall support plain text and pre-defined advisory templates. Acknowledgement receipt shall be tracked and displayed to the sender.	Broadcast Notifications with ACK
<b>FR-AUD-016</b>	The system shall integrate with the NHAI radio communications and PTT (Push-to-Talk) system, enabling operators to initiate radio calls to patrol	PTT / Radio Integration

Req ID	Requirement Description	Sub-Module / Feature
	units directly from within the incident record, with the call linked automatically to the incident timeline.	
<b>FR-AUD-017</b>	The communication module shall provide a contacts directory accessible from any operator workstation, listing all registered stakeholders (ambulance services, police stations, NHAI officials, agency contacts) with their communication details, categorised by corridor and role. The directory shall be manageable by System Administrators.	Stakeholder Contacts Directory

#### 9.4.5. Module 5 — Report Generation Module and Dashboard

1. This module shall generate periodic as well as on-demand statistical reports using data received from VIDES, TMCS, Automatic Traffic counter cum Classifier (ATCC) for traffic planning and management, as well as traffic forecasting. There shall also be a provision to generate reports to aid planning and strategizing enforcement.
2. While tabular reports are necessary, the software shall include visually appealing and useful dashboards and charts for efficient day to day management, monitoring and operations.
3. Further, the Database/Data Analyst in the ATMS shall on their initiative and on request conduct statistical analysis on the data being generated and provide insights to the manager and NHAI PD on a monthly basis.
4. The reporting module shall provide a range of reports on demand including those:
  - related to the acquired data,
  - VMS messages edited and sent,
  - System generated Equipment availability and downtime.
  - System malfunction and restoration
  - User login – logout
  - Daily Accidents that happened on the highway and their action taken report.
  - Manually detected and Automatic VIDES events detected by location, vehicle type, and action taken, end to end response time etc.
  - E-Challans generated (manual vs automatic) and sent to Vaahan.
  - Mobile App messages received
  - Traffic flow volume (No of vehicles detected during the time interval), Occupancy (Lane occupancy measure in percentage of time), Vehicle classification, Flow rate (vehicle per hour per lane), Headway (Average time interval between two vehicles), Speed, Level of Service, Space occupancy & Traffic Density from both the ATCC and the VIDS data captured from the respective field equipment.
5. The ATMS Software shall have provision to select end of day reports through API automatically to NHAI's Data Lake or equivalent.
6. The module shall further provide detailed performance reports on all aspects ranging from detection of incidents,

through the field Operations team (Patrol vehicles, Break-down cranes and Ambulances) actions, Traffic Management Console operator and other ATMS Control Centre operator actions. Automatic system generated reports supporting the service provider's claim of meeting the service level requirements with respect to operations, shall also be provided.

7. The Report Generation Module will ensure that all the metrics mentioned in the SLA are easily available and automatically generated. In case manually verification of random footage is required in SLA calculation, the reporting module will provide easy module to fetch footage in any time period/equipment as needed. Detailed formats of each report shall be finalised by the LCCC Service Provider in consultation with IHMCL.

The system shall provide detailed reports related to the System Operations (including the actions of various stakeholders during Incident Management) and operations. The format shall be finalized by the service provider in consultation with NHAI/IHMCL during project implementation and O&M period.

Maintenance reports, at minimum, shall include the current operational status of each equipment, actual events of down-times, actual events of Mean Time To Repair (MTTR) of each equipment, actual events of Mean time between Failure (MTBF) of each equipment, and the preventive and repair maintenance log with Root Cause Analysis (RCA) report. The system shall also provide a method to log and report road highway incidents.

Further the system shall provide a facility of generating user-formatted reports that can bring together the occurrence of highway incidents, values of various sensors and the operational status of various equipment on a common time line/scale.

#### 9.4.5.1. *Role-Specific Operational Dashboards*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-RPT-001</b>	The system shall provide role-specific operational dashboards for: LCCC operators (corridor-level — incidents, device health, weather, active SOPs), RCCC supervisors (regional-level — inter-corridor comparison, regional SLA, escalation queue), NCCC managers (national-level — programme KPIs, cross-regional incident map, national device availability), and NHAI/MoRTH leadership (programme-level — safety outcomes, enforcement revenue from vendor feed, system availability, investment performance). All dashboards shall be widget-based, configurable per user, and auto-refreshed.	Role-Specific Dashboards



Req ID	Requirement Description	Sub-Module / Feature
<b>FR-RPT-002</b>	The system shall provide a KPI Framework enabling authorised administrators to define: KPI name, description, data source (ATMS-native or vendor feed), calculation formula, measurement unit, reporting frequency, warning threshold, critical threshold, baseline target, and responsible owner. An unlimited number of custom KPIs shall be configurable.	Configurable KPI Framework
<b>FR-RPT-003</b>	All KPIs shall be displayed using standardised colour-coded indicators: Green (within acceptable limits, no action required), Yellow (cautionary — monitoring required, corrective action may be necessary), Red (critical — threshold breached, immediate action required). KPI status shall update in real time. Drill-down shall be available from any KPI tile to the underlying operational data.	KPI Colour Coding & Drill-Down
<b>FR-RPT-004</b>	The system shall provide time-series trending charts for all KPIs and key operational metrics over user-defined periods from 1 hour to 5 years. Charts shall support overlaying multiple metrics on the same time axis for correlation analysis.	KPI Trending & Time-Series
<b>FR-RPT-005</b>	The KPI framework shall support ITIL (IT Infrastructure Library) standards for Standard Operations Plan and Resource Management, and shall support BPMN (Business Process Model and Notation) or equivalent for the design, configuration, and visualisation of KPI monitoring workflows.	ITIL & BPMN Alignment

#### 9.4.5.2. Pre-Built Automated Report Library

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-RPT-006</b>	The system shall generate a daily operations summary report for each LCCC, RCCC, and NCCC at 00:00 hours (IST) covering: incidents by type and severity with SLA compliance, VMS advisory requests made and their status (from vendor VMS platform), device health summary (ATMS-managed devices and summary from vendor platform telemetry),	Daily Operations Summary

Req ID	Requirement Description	Sub-Module / Feature
	weather events and threshold breaches, 1033/ECB call volume, and ANPR reads and violation counts (from vendor feed).	
<b>FR-RPT-007</b>	The system shall generate weekly enforcement revenue reports for IHMCL: challans generated by type, challans settled, revenue collected (MTD and YTD), outstanding challans, dispute rate, and top violation corridors. All data sourced from the Existing Field Platform Vendor's e-Challan system via API feed. The system shall generate weekly challans by corridor including: repeat offenders, vehicles by fleet owner (where master data is provisioned), repeat offence types and circulate the list to LCCC/RCCC/Police and other stakeholders for future preventive action.	Weekly Enforcement Revenue
<b>FR-RPT-008</b>	The system shall generate monthly SLA performance reports per TSP and per ATMS project: device availability by device type (ATMS-managed devices and vendor-reported devices separately), fault count and MTTR (Mean Time to Repair), MTBF (Mean Time Between Failure), SLA breaches, financial penalty computation, and open vs. closed maintenance ticket count.	Monthly SLA Performance
<b>FR-RPT-009</b>	The system shall generate an annual programme performance report for MoRTH and NHAI covering: safety improvement trends (incident rate per 100 MVKM), fatality rate trend, enforcement revenue (from vendor), SLA compliance trend, system availability, predictive analytics accuracy summary, and investment performance indicators.	Annual Programme Report
<b>FR-RPT-010</b>	The system shall generate shift handover reports at each configured shift change, automatically distributed to the incoming operator. The report shall include: active incidents with current status, open alarms and pending SOP tasks, device faults in progress, active geofence alerts, and weather alerts.	Shift Handover Report
<b>FR-RPT-011</b>	The system shall generate maintenance reports including: current operational status of each equipment item, actual events of downtimes (by device, by corridor, by TSP), actual events of MTTR per device type, actual events of MTBF per device type, and preventive and repair maintenance log with technician attribution.	Maintenance Reports
<b>FR-RPT-012</b>	The system shall generate NHAI ATMS Policy compliance dashboards showing KPI actuals vs. policy targets per corridor, updated monthly and available to NHAI leadership on demand.	Policy Compliance Dashboard

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-RPT-013</b>	The system shall produce CERT-In cybersecurity compliance reports on demand, covering: MFA adoption rate, vulnerability scan status, patch compliance percentage (by CVE severity), security incident count, and SIEM alert resolution rate.	Cybersecurity Compliance Report

#### 9.4.5.3. Custom Reporting and Distribution

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-RPT-014</b>	The system shall provide a report builder enabling authorised users to configure custom reports by selecting: data domains (incidents, devices, enforcement, weather, SLA), date/time range filters, geographic filters (national/regional/corridor), grouping dimensions, aggregation functions, and visualisation types (bar, line, pie, table, heat map). Custom reports shall be saveable and shareable within the same tier.	Custom Report Builder
<b>FR-RPT-015</b>	All reports (pre-built and custom) shall support scheduling for automated generation and email distribution: daily, weekly, monthly, and quarterly. Distribution lists shall be configurable per report type, with per-recipient format selection (PDF, Excel, CSV).	Automated Scheduling & Distribution
<b>FR-RPT-016</b>	All reports shall be exportable in PDF (formatted, print-quality), Excel (XLSX with separate tabs per data domain), and CSV formats. PDF exports shall include the NHAI logo, report generation timestamp, user ID, and classification marking.	Report Export Formats
<b>FR-RPT-017</b>	The system shall provide an ad-hoc query and report builder interface for authorised Data Analyst users, allowing SQL-free custom queries across all data lake tables using a guided query builder. Results shall be visualisable as charts or downloadable as CSV.	Ad-Hoc Query Builder
<b>FR-RPT-018</b>	The system shall provide a report favourites list enabling operators to bookmark frequently used reports for rapid one-click access from the dashboard.	Report Favourites
<b>FR-RPT-019</b>	The system shall provide API access to all analytical datasets for authorised external systems using OpenAPI 3.0-compliant REST endpoints, documented via a developer portal. Data returned via API shall	Analytics API Access

Req ID	Requirement Description	Sub-Module / Feature
	follow the canonical data schema and include metadata fields (report generation time, data freshness timestamp, schema version).	
<b>FR-RPT-020</b>	The system shall perform automated end-of-day push of all ATMS operational data to NHAI DataLake/ERP via a scheduled API call in the standardised NHAI format. Push success/failure shall be logged and alerted to the System Administrator.	DataLake End-of-Day Push

#### 9.4.6. Module 6 — System Administration Module

This module shall essentially enable the definition and maintenance of user accounts. It shall be possible to control / restrict all functions / sub-functions available in each module based on the user group; access control shall have 3 levels of access: Read, Write, and Modify. All manual override options shall be separate functions that can be disabled for any user/user group. At the end of session, the operator logs out and the logout shall be recorded in the database. It shall not be possible for a different user to open a separate instance of the application without the current user logout on the same workstation. It shall be possible to exit the application only with Administrator authentication.

##### 9.4.6.1. User Identity and Authentication

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-USR-001</b>	The system shall implement Multi-Factor Authentication (MFA) as mandatory for all user logins across all tiers, tiers and all access methods (web, mobile, API). Approved MFA methods: TOTP authenticator app (preferred), hardware security key (FIDO2/WebAuthn), and OTP via SMS (fallback only — not permitted as sole MFA factor for P1 access roles).	MFA — All Users
<b>FR-USR-002</b>	The system shall support Single Sign-On (SSO) via SAML 2.0 or OpenID Connect for integration with the NHAI/MoRTH enterprise identity provider. Active Directory / LDAP integration shall be supported for synchronisation of user accounts, with AD group memberships used to auto-assign ATMS roles at first login, subject to administrator confirmation.	SSO & LDAP/AD Integration
<b>FR-USR-003</b>	User accounts shall be locked after 5 consecutive failed login attempts. Locked accounts shall require authorisation from a System Administrator to unlock. All lockout events shall be alerted to the SIEM and to the System Administrator in real time.	Account Lockout Policy

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-USR-004</b>	Active user sessions shall be automatically terminated after a configurable inactivity period (default: 15 minutes for operator workstations, 5 minutes for mobile devices, 30 minutes for leadership dashboards). The operator shall receive a 2-minute warning before automatic session termination.	Session Timeout & Warning
<b>FR-USR-005</b>	Password policies shall comply with CERT-In guidelines: minimum 12 characters, mandatory complexity (uppercase, lowercase, numeric, special character), maximum 90-day expiry, password history preventing reuse of last 12 passwords, and prohibition of dictionary words or sequential patterns.	Password Policy (CERT-In)
<b>FR-USR-006</b>	It shall not be possible for a different user to open a separate instance of the application without the current user logging out on the same workstation. The system shall detect and prevent concurrent sessions from the same user account on different workstations unless explicitly permitted by the administrator for supervisory roles.	Session Integrity
<b>FR-USR-007</b>	Exiting the ATMS application from any workstation shall require Administrator authentication (username + password/MFA). This requirement shall apply even if the current session user is an operator, preventing unauthorised shutdown of operational systems.	Exit Authentication

#### 9.4.6.2. *Role-Based Access Control (RBAC)*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-USR-008</b>	The system shall implement RBAC with three access levels for every function, data object, and API endpoint: Read (view only), Write (create/submit), and Modify (edit existing records). Access control lists shall be enforceable at the field level within forms (e.g., an operator can view but not modify certain fields on an incident record).	Three-Level RBAC
<b>FR-USR-009</b>	The platform shall support a minimum of 12 pre-defined user roles with the ability for administrators to create unlimited custom roles. Pre-defined roles shall be as specified in the Role Table in Section 7.8.2.1. All roles shall be configurable by the System Administrator without system restart.	Pre-Defined & Custom Roles

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-USR-010</b>	User accounts shall be associated with a jurisdictional scope (national / regional / corridor). Data visibility, GIS map extent, incident scope, report scope, and all search results shall be automatically limited to the user's assigned jurisdiction. Jurisdictional scope shall be enforced at the data access layer, not only in the UI.	Jurisdictional Data Scoping
<b>FR-USR-011</b>	All manual override options (e.g., overriding SLA escalation, bypassing SOP mandatory steps, overriding automated VMS advisory request) shall be implemented as separate permissions that can be individually enabled or disabled per role without affecting other functions.	Manual Override Permission Control
<b>FR-USR-012</b>	All RBAC access denied events shall be logged to the audit trail with: attempted action, user ID, resource requested, timestamp, and workstation. The system shall alert the Security Administrator if any user accumulates more than 10 access-denied events within 1 hour.	Access Denied Logging & Alerting
<b>FR-USR-013</b>	Administrators shall be able to create, modify, clone, and deactivate user accounts and roles through the user management console. Deactivated accounts shall be retained in the system for audit purposes with all historical activity preserved.	Account & Role Lifecycle Management

#### 9.4.6.3. Standard User Role Definitions

Role	Tier	Primary Permissions
<b>National Programme Director</b>	NCCC	Read-only access to all dashboards and reports; no operational controls; leadership dashboard access
<b>NCCC Supervisor</b>	NCCC	Full NCCC operational controls; cross-regional escalation; national broadcast; manual override for Major/Catastrophic
<b>NCCC Operator</b>	NCCC	National monitoring; incident escalation initiation; national GIS view
<b>RCCC Supervisor</b>	RCCC	Full RCCC controls; LCCC remote view; regional VMS advisory requests; incident escalation to NCCC
<b>RCCC Operator</b>	RCCC	Regional monitoring; incident management; regional VMS advisory; SOP task execution
<b>LCCC Supervisor</b>	LCCC	Full corridor operational controls; SOP approval; VMS advisory approval; incident closure approval (Major+)

Role	Tier	Primary Permissions
<b>LCCC Operator</b>	LCCC	Corridor monitoring; incident management; SOP task execution; VMS advisory request; ERSS 112/1033/ECB communication
<b>Enforcement Officer</b>	LCCC/RCCC	Violation review (vendor data); challan lifecycle monitoring; dispute management interface; watch-list query
<b>System Administrator</b>	All	User management; RBAC configuration; device registry; alert thresholds; SOP library; audit log access; system configuration
<b>Data Analyst</b>	NCCC/RCC	Analytics; reporting; ad-hoc queries; data export; no operational controls
<b>Contractor / TSP Portal</b>	Portal	SLA data and maintenance tickets for own contract scope only (read-only); evidence submission
<b>Police Liaison</b>	LCCC/RCCC	Enforcement records (from vendor); incident reports; watch-list view; restricted CCTV stream token access
<b>PIU / Regional Office</b>	Portal	Read-only dashboard for assigned project corridors; weekly/monthly report export
<b>Disaster Management Liaison</b>	NCCC/RCCC	Emergency incident feed; corridor status view; no write access
<b>Incident Response Teams cross departments (RCCC/ LCCC/ Police/ DM)</b>	Mobile App/ iCAD	Receive incoming incident details and SOPs; submit evidence or incident report specific to their SLA either via mobile app or via integration/ iCAD

#### 9.4.6.4. System Configuration Management

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SYS-001</b>	The System Administration console shall enable authorised administrators to configure, without requiring vendor support: device registry management (add/edit/deactivate devices), alert threshold values (per device type, per corridor), SOP library (create/edit/version/deactivate), geofenced zone management, data ingestion pipeline configuration, and user/role management.	System Admin Console Functions



Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SYS-002</b>	All configuration changes made through the System Administration console shall be logged to an immutable configuration audit trail with: administrator user ID, timestamp, changed parameter name, old value, new value, and change justification (mandatory free-text field).	Configuration Audit Log
<b>FR-SYS-003</b>	The system shall support automated backup at intervals not exceeding 24 hours for all configuration data, user data, and operational data. Recovery Point Objective (RPO) shall be 4 hour for critical operational data (incidents, SOP states, audit logs). Recovery Time Objective (RTO) for full system restoration shall not exceed 2 hours. DR testing shall be conducted quarterly with results documented.	Backup, RPO, and RTO
<b>FR-SYS-004</b>	The system shall operate 24×7×365 across all command tiers. Planned maintenance windows shall be permissible only at NCCC-approved times with prior 72-hour notice to all RCCC supervisors. Emergency maintenance shall be documented with post-maintenance report to NHAI/IHMCL within 24 hours.	Continuous Operation & Maintenance Windows
<b>FR-SYS-005</b>	The system shall support concurrent operation of 1 NCCC, 20+ RCCs, and 667+ LCCs with data flowing across all tiers simultaneously without performance degradation. The system shall support a minimum of 100,000 simultaneously connected field devices.	Multi-Tier Scale
<b>FR-SYS-006</b>	LCCC deployments shall support autonomous operation for a minimum of 168 hours during WAN outage using local data buffering. All locally actioned incidents, SOP tasks, 1033 calls, and device fault events shall be preserved and synchronised to the national data lake automatically upon WAN restoration, in correct chronological sequence.	LCCC Autonomous Operation
<b>FR-SYS-007</b>	The system shall be cloud ready. The system shall be deployed at NCCC on-premises with cloud virtualization supporting containerised deployment via Kubernetes with Infrastructure-as-Code (IaC) provisioning (Terraform or equivalent). Deployment scripts shall be version-controlled and reproducible. The NCCC shall have DR with MEITY-empanelled cloud infrastructure (public/private/hybrid).	Cloud-Native Deployment K8s
<b>FR-SYS-008</b>	The software shall not be subject to OEM licensing restrictions limiting scalability across additional processors, cores, VMs, or physical servers. The system shall support unrestricted horizontal and vertical scaling without license renegotiation.	License-Unrestricted Scalability

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SYS-009</b>	No proprietary communication protocols shall be used between system components and field devices. Where a proprietary protocol is technically unavoidable for a specific device integration, complete technical documentation, interface specifications, and source code (where applicable) shall be submitted to IHMCL/NHAI. All such exceptions shall be documented and approved by the IHMCL Programme Office.	No Proprietary Protocols Policy
<b>FR-SYS-010</b>	The system shall provide a system health dashboard visible to the System Administrator showing: application server CPU/memory/disk utilisation (per node), database connection pool status, ingestion pipeline throughput, queue depths, LCCC WAN connectivity status for all LCCCs, and last successful DR replication timestamp.	System Health Dashboard

#### 9.4.7. Module 7 — Communication Module for Authorised Access by External Systems

Communication module for authorized access by external systems (e.g. NHAI's Regional control centre & the Main control centre). This module will manage authorized access to the ATMS system by:

- Authorized NHAI personnel/representatives;
- Other authorized NHAI systems like the Regional office Control Centre ATMS system and the Main Control centre ATMS system;
- Any other system authorized by NHAI. Based on requests from the above entities the communication module shall provide the following information to the requesting entity:
  - Video Streams (Live and Archived);
  - Audio streams (Live and Archived);
  - Data strings and Data elements (Live and Archived).
- The standard data exchange protocols for the above will be shared by NHAI/IHMCL with the Service Provider.

##### 9.4.7.1. Authorised External Access Management

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-COM-001</b>	The system shall manage authorised access to the ATMS platform by: (a) NHAI/IHMCL personnel at NCCC/RCCC/LCCC; (b) NHAI Regional Office control centres; (c) NHAI HQ Master Control Centre; (d) State Integrated Command and Control Centres (ICCCs); (e) Traffic Police PCR (Police	Authorised Access Entities

Req ID	Requirement Description	Sub-Module / Feature
	Control Room); (f) PIU/RO portal users; (g) Disaster Management Centre (DMC/SDMA); (h) Any other entity authorised by NHAI via a formal onboarding process.	
<b>FR-COM-002</b>	The communication module shall provide authorised entities with the following data, subject to their RBAC permissions: (a) Live and archived structured data strings and data elements (incident records, device health, weather, traffic); (b) Audio streams — live and archived call recordings from the integrated audio communication module; (c) Video stream access tokens for CCTV/TMCS feeds, sourced from the Existing Field Platform Vendor's system and routed through the ATMS API layer with access logging.	Data/Audio/Video Provision to Entities
<b>FR-COM-003</b>	A centralised National API Gateway shall enforce: OAuth 2.0 / API key authentication (per external entity), role-mapped access scopes, rate limiting (configurable per entity), API versioning (minimum 2 concurrent major versions supported), full transaction logging (request, response code, latency, entity ID, timestamp), and anomaly detection (sudden volume spike or unusual data request patterns shall trigger a security alert).	National API Gateway Controls
<b>FR-COM-004</b>	The system shall provide a Police PCR dedicated video feed interface over an P2P/Managed MPLS or OFC-based dedicated circuit (not over the public internet). The interface shall support: RTSP live stream access tokens for cameras in the police jurisdiction; HTTP snapshot pull at up to 1 frame-per-second per camera; role-based permission model restricting Police stream access to their jurisdictional corridor cameras only.	Police PCR Dedicated Network Feed
<b>FR-COM-005</b>	The system shall provide a read-only PIU/Regional Office (RO) Dashboard accessible via a dedicated secure portal login. The dashboard shall display: project-level device health status, daily incident count and type summary, enforcement summary (from vendor e-Challan feed), ANPR read accuracy (from vendor feed), and SLA compliance for all LCCCs within the PIU/RO jurisdiction. Access shall be restricted to assigned corridors only.	PIU/RO Read-Only Dashboard
<b>FR-COM-006</b>	PIU/RO dashboard users shall be able to export weekly and monthly operational summary reports in PDF and Excel formats. All exported reports shall be watermarked with the user's identity, export timestamp, and 'RESTRICTED' classification marking.	PIU/RO Report Export with Watermark

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-COM-007</b>	The system shall integrate with State ICCCs for bi-directional event sharing using a defined event exchange API. The ATMS Platform shall push highway incidents $\geq$ Moderate to the State ICCC within 2 minutes of classification and receive State ICCC events that affect the national highway corridor.	State ICCC Bi-Directional Integration
<b>FR-COM-008</b>	The system shall expose a DATEX II Version 3.2-compliant data feed for international data exchange and alignment with international traffic management standards. The DATEX II feed shall cover: incident data, traffic conditions, weather conditions, and VMS advisory status.	DATEX II v3.2 Compliance Feed
<b>FR-COM-009</b>	The system shall integrate with State and National Disaster Management Centres (DMC/SDMA) via the NDMA data exchange framework: (a) real-time push of highway emergencies $\geq$ Major within 2 minutes of classification (incident type, GPS, type, estimated casualties, resources dispatched, estimated clearance time); (b) corridor status feed (open/restricted/closed) updated every 15 minutes; (c) pull API for DMC on-demand corridor status query.	DMC/SDMA Integration
<b>FR-COM-010</b>	The DMC/SDMA integration API shall use the NDMA-defined highway emergency data schema (or MoRTH-approved equivalent). All schema fields shall be documented in the System Integration Register and approved by IHMCL/NHAI before go-live.	DMC Integration Data Schema
<b>FR-COM-011</b>	The system shall maintain an API integration health dashboard showing for every external integration: connection status (live/degraded/offline), last successful transaction timestamp, transaction volume (hourly/daily), error rate, and average response time. The dashboard shall be accessible by both System Administrators and NHAI programme managers.	Integration Health Dashboard
<b>FR-COM-012</b>	The system shall comply with applicable e-Governance standards, frameworks, policies, and guidelines issued by the Government of India (MeitY, NIC, CERT-In) to ensure interoperability, security, and regulatory compliance. The System Integration Register shall document compliance status for each standard.	e-Governance Compliance

**9.4.8. Module 8 — API Integrations (VAHAN, CCTNS, NPCI FASTag, NHAI ERP/DataLake, 1033 CAD, Rajmarg, and Existing Field Platform Vendor and other third party DBs as and when required)**

API Integrations with Vaahan, NPCI FASTag Mapper, NHAI's ERP (Datalake at the time of this notice), 1033 CAD, Rajmarg etc. ATMS software shall be required to be integrated with IT systems from NHAI or other Government Agencies from time to time. This shall be possible at no additional cost whether during installation or O&M phase of the contract. / NHAI/IHMCL shall provide necessary support, coordination, and access to relevant systems, APIs, and documentation required for integration. However, the overall responsibility for successful integration, including development, testing, commissioning, and ensuring seamless interoperability, shall rest solely with the System Development Agency (SDA).

Any delays, failures, or performance issues arising out of integration shall be the responsibility of the SDA.

#### 9.4.8.1. Government & National System Integrations

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INT-001</b>	The system shall integrate with VAHAN (National Vehicle Registry) through the NIC API gateway to enable real-time vehicle record queries. Queries shall return: registered owner name and address, vehicle class, make/model, registration validity date, insurance validity date, fitness certificate validity, and PUC certificate validity. The system shall cache VAHAN responses for configurable durations to manage API rate limits without compromising data freshness.	VAHAN Integration
<b>FR-INT-002</b>	The system shall integrate with SARATHI (Driving Licence Registry) to retrieve: driver name, licence category, licence validity date, endorsements, and penalty point records. SARATHI data shall be used for enforcement reporting and repeat offender tracking by the reporting module.	SARATHI Integration
<b>FR-INT-003</b>	The system shall integrate with FASTag / NETC (NPCI FASTag Mapper) for bi-directional data exchange: (a) receiving toll transaction confirmations for vehicles on the corridor; (b) transmitting toll evasion alerts flagged by the vendor ANPR system (vehicle passage confirmed but no corresponding FASTag transaction). Integration shall use NPCI's published API standards.	FASTag / NETC Integration
<b>FR-INT-004</b>	The system shall integrate with the NIC Enforcement Portal to receive e-challan transmission status and settlement updates originating from the Existing Field Platform Vendor's enforcement module. ATMS shall maintain a challan status register updated from the NIC portal for reporting and analytics.	NIC Enforcement Portal

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INT-005</b>	The system shall integrate with the eCourts (NJDG) system for transmission of defaulted challan records (sourced from vendor enforcement data, confirmed by NIC portal status) for court proceedings. Transmission shall be automated upon a configurable defaulted-challan age threshold.	eCourts / NJDG Integration
<b>FR-INT-006</b>	The system shall integrate with DigiLocker for secure digital storage and sharing of enforcement evidence. Evidence (images, video clips) originates in the vendor enforcement module; ATMS manages the DigiLocker linkage enabling vehicle owners to download their challan evidence via the DigiLocker platform.	DigiLocker Integration
<b>FR-INT-007</b>	The system shall integrate with CCTNS (Crime and Criminal Tracking Network and Systems) to enable: vehicle verification by number plate (ANPR data forwarded from vendor), real-time blacklist/stolen vehicle checking, incident-to-police-record linking, and e-Challan data sharing with enforcement systems.	CCTNS Integration
<b>FR-INT-008</b>	The system shall integrate with PM Gati Shakti to share: real-time traffic condition data (from vendor ATCC/VIDS feed), incident events, ATMS asset locations, and road condition data. Integration shall conform to the PM Gati Shakti data exchange standards.	PM Gati Shakti Integration

#### 9.4.8.2. *Emergency Services and Operational Integrations*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INT-009</b>	The system shall integrate with ERSS 112 (Emergency Response Support System) to automatically transmit Major and Catastrophic incident notifications within 2 minutes of incident classification. Notification payload shall include: GPS coordinates, incident type, severity, estimated number of casualties, highway name, nearest KP, and current weather at incident location.	NERS 112 Integration
<b>FR-INT-010</b>	The system shall integrate with the 1033 iCAD (Integrated Computer Aided Dispatch) system. Integration shall support: (a) incidents identified by 1033 operators communicated to ATMS via API with full incident attributes; (b) ATMS dispatches emergency vehicles (RPV, Ambulance, Crane etc.) through iCAD and receives real-time vehicle tracking updates;	1033 iCAD Integration

Req ID	Requirement Description	Sub-Module / Feature
	(c) incident closure notifications sent from ATMS back to iCAD. Integration shall be bidirectional.	
<b>FR-INT-011</b>	The system shall integrate with the Rajmarg Yatra mobile platform: (a) ATMS receives crowd-sourced incident reports with location (GPS), photo, and incident type via the Rajmarg API — nearest TMCS camera is auto-identified for operator confirmation; (b) ATMS sends traffic, congestion, maintenance work, and incident advisories (geo-tagged) to Rajmarg Yatra users in the incident vicinity; (c) event closure notifications are sent to Rajmarg when an incident is resolved.	Rajmarg Yatra Integration
<b>FR-INT-012</b>	The system shall integrate with the official NHAI Mobile App (NHA App) to provide: live traffic condition data per corridor (from vendor ATCC/VIDS feed), incident notifications with estimated clearance time, VMS message replication (current message from vendor VMS platform), travel advisory push notifications, and highway helpline 1033 click-to-call integration. Data exchange format shall conform to MoRTH open data standards.	NHA Mobile App Integration
<b>FR-INT-013</b>	The system shall integrate with state police dispatch systems for electronic handover of enforcement records (sourced from vendor e-Challan system) and watch-list vehicle alerts (from vendor ANPR system). Police stream access shall be provided via the dedicated PCR network feed (FR-COM-004).	Police Dispatch Integration
<b>FR-INT-014</b>	The system shall provide API integration with ambulance and fire service dispatch systems to enable resource mobilisation requests directly from the ATMS incident management module. Dispatch requests shall include: incident GPS location, incident type, severity, number of persons involved (if known), and current weather conditions.	Ambulance / Fire Dispatch Integration
<b>FR-INT-015</b>	The system shall integrate with the Indian Meteorological Department (IMD) API to receive national and corridor-level weather forecasts at configurable intervals (default: every 3 hours). IMD forecast data shall be fused with real-time AWS sensor data and displayed as a combined weather layer on the GIS map, with measured and forecast conditions clearly distinguished.	IMD Weather Integration
<b>FR-INT-016</b>	The system shall integrate with the AIS-140 vehicle tracking platform (or equivalent government-approved GNSS-based vehicle tracking	AIS-140 Vehicle Tracking



Req ID	Requirement Description	Sub-Module / Feature
	standard) to receive real-time GPS location of all registered highway patrol vehicles, ambulances, and cranes assigned to ATMS project corridors.	

#### 9.4.8.3. Existing Field Platform Vendor API (Core Integration)

All interfaces with the Existing Field Platform Vendor are governed by a formal Data Exchange Specification (DES) agreed between NHAI/IHMCL, the ATMS SDA, and the Existing/Onboarded Field Platform Vendor. Standard format: JSON/XML over HTTPS REST or MQTT. Authentication: OAuth 2.0/API key. Interface versions tracked in the System Integration Register.

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-INT-017</b>	The system shall receive structured incident detection events from the Existing Field Platform Vendor's VIDES/TMCS system within 5 seconds of the detection event. Each event shall include: incident type, camera ID, KP, corridor ID, severity (as classified by VIDES AI), confidence score, thumbnail image URL, and bounding box metadata. The interface shall be bidirectional: ATMS sends incident acknowledgement and closure back to the vendor platform.	VIDES/TMCS Event Feed
<b>FR-INT-018</b>	The system shall receive from the vendor ANPR/VSDS/TTMS system: vehicle passage records (plate, class, camera ID, KP, direction, lane, timestamp, speed where available), journey time computations per ANPR pair, average speed per segment, and speed violation flags. Data shall be received at intervals not exceeding 60 seconds for aggregate feeds and within 10 seconds for individual violation events.	ANPR/VSDS/TTMS Data Feed
<b>FR-INT-019</b>	The system shall receive VMS device status and current displayed message content from the vendor VMS system at intervals not exceeding 60 seconds. ATMS may send advisory message requests to the vendor VMS system upon incident confirmation or weather threshold breach, subject to the agreed interface protocol.	VMS Status & Advisory Interface
<b>FR-INT-020</b>	The system shall receive e-challan violation records and full challan lifecycle status from the Existing Field Platform Vendor's enforcement module for ATMS reporting, analytics, PIU/RO dashboards, and regulatory	e-Challan Lifecycle Feed

Req ID	Requirement Description	Sub-Module / Feature
	compliance. Status updates shall be received within 5 minutes of each state change in the vendor system.	
<b>FR-INT-021</b>	The system shall receive device health telemetry from the vendor NMS for VIDES cameras, ANPR cameras, VMS units, and speed radars. This telemetry shall feed the ATMS SLA computation engine and the Asset Lifecycle dashboard.	Vendor NMS Health Telemetry Feed
<b>FR-INT-022</b>	The system shall support an Open Data / Developer Portal provisioning project data (both static and real-time) in open formats: GeoJSON, CSV, and OpenAPI 3.0-compliant REST endpoints. The portal shall support integration with the IHMCL Future Open Data developer portal, enabling secure and standardised data access for authorised stakeholders and third-party developers.	Open Data / Developer Portal
<b>FR-INT-023</b>	All external and vendor API integrations shall comply with applicable e-Governance standards and frameworks issued by the Government of India to ensure interoperability, security, and regulatory compliance. All data sharing shall be facilitated through well-defined, interoperable, documented interfaces accessible through a secure web portal and/or standardised API services.	e-Governance Integration Standards

#### 9.4.9. Module 9 — Real-Time Equipment Health Monitoring / Network Management System (NMS)

Network Management Software. The Solution should provide fault & performance management of the infrastructure and should monitor IP/SNMP etc. enabled devices like Cameras, Routers, Switches, ATMS Software, Emergency Call Boxes, Sensors, etc. (i.e., all devices supplied as part of ATMS scope). This system shall also help monitor key KPI metrics like availability, in order to measure SLAs. It shall include key functionalities to assist administrators to monitor network faults, uptime & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore equipment services. The Contractor will provide a real-time dashboard for monitoring equipment/network for which NHAI will have access to check and monitor SLAs at any time. The NMS should ensure that the items mentioned in the SLA in Annexure are automatically calculated and reported in the requisite format thereby making it easy to monitor SLAs at a glance.

##### 9.4.9.1. Asset Registry

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-NMS-001</b>	The system shall maintain a comprehensive asset registry for every field device within ATMS scope: device ID (unique globally), device type, manufacturer, model, hardware version, firmware version, serial number, installation date, installation KP, ATMS project corridor, contracted TSP, warranty expiry date, expected service life, and current operational status. The registry shall be displayed on the GIS map with device-type icons.	Asset Registry
<b>FR-NMS-002</b>	The asset registry shall track full lifecycle history per device: commissioning date, all software/firmware upgrades (with version history), all fault events (with timestamps and duration), all maintenance visits (with technician, action taken, and parts replaced), and device retirement/replacement. Lifecycle history shall be retained for the life of the contract.	Asset Lifecycle History
<b>FR-NMS-003</b>	The system shall support bulk asset import and update via CSV template or API for initial commissioning of large device populations (e.g., 500 cameras in a new corridor). A bulk import validation report shall identify errors before committing data.	Bulk Asset Import
<b>FR-NMS-004</b>	The system shall provide an asset lifecycle dashboard showing: total assets by type and status, assets approaching end-of-life (within 12 months based on expected service life), warranty expiry alerts (60 days advance warning), cumulative fault rate per asset type per corridor, and MTBF trend per asset type.	Asset Lifecycle Dashboard

#### 9.4.9.2. *Real-Time Device Health/Status Monitoring*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-NMS-005</b>	The system shall provide continuous real-time monitoring of all IP/SNMP-enabled infrastructure devices in ATMS scope: Automatic Weather Stations (AWS), Emergency Call Boxes (ECBs), UPS units, routers, switches, fibre transceivers, ATMS edge servers, and WAN link endpoints. Monitoring shall include: connectivity status, CPU utilisation, memory utilisation, interface traffic (Mbps), error rates, and power status.	Infrastructure Device Monitoring

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-NMS-006</b>	The system shall generate an automated fault alert within 60 seconds of any managed device going offline, reporting a degraded state, or exceeding configured performance thresholds. Fault alerts shall be classified by severity (Critical/Major/Minor) and automatically trigger a maintenance ticket creation.	Fault Alerting — 60-Second SLA
<b>FR-NMS-007</b>	The system shall monitor connectivity link performance for all LCCC corridors: latency, packet loss, jitter, and available bandwidth. WAN degradation alerts shall be generated when link performance falls below configured thresholds. Connectivity performance trend charts shall be available per corridor.	WAN Link Performance Monitoring
<b>FR-NMS-008</b>	The system shall aggregate and display device health telemetry received from the Existing Field Platform Vendor's NMS (for VIDES cameras, ANPR cameras, VMS units, speed radars). Vendor-reported device status shall be displayed on the ATMS GIS map and included in SLA computation, clearly attributed as 'vendor-reported' data.	Vendor Device Health Aggregation
<b>FR-NMS-009</b>	The system shall provide an availability heatmap per corridor and per region, showing real-time device availability percentage segmented by device type. The heatmap shall be accessible from both the NMS dashboard and the NCCC/RCCC operational GIS dashboards.	Availability Heatmap
<b>FR-NMS-010</b>	The system shall implement a predictive maintenance model identifying field devices with elevated failure probability based on: device age, fault history, firmware version age, operating environment (AWS temperature/humidity), and MTBF statistics for the same device model. Predicted high-risk devices shall be surfaced in the SLA management module as preventive maintenance recommendations.	Predictive Maintenance Model

#### 9.4.9.3. SLA Monitoring and Penalty calculation

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-NMS-011</b>	The system shall automatically compute SLA compliance metrics for each contracted KPI from system-generated operational data without manual data entry: device availability per device/corridor/TSP (daily/weekly/monthly), fault MTTR per device type, incident response	Automated SLA Computation

Req ID	Requirement Description	Sub-Module / Feature
	time (from ATMS incident engine), and — based on vendor telemetry — ANPR accuracy, VMS uptime, and video availability (as reported by vendor platform).	
<b>FR-NMS-012</b>	The system shall track device downtime with millisecond precision: every fault event is timestamped at automatic detection and at technician-confirmed restoration. The downtime duration feeds directly into the availability percentage computation without manual data entry.	Precision Downtime Tracking
<b>FR-NMS-013</b>	The system shall alert the responsible TSP and the NHAI contract manager when device availability for any corridor falls below 80% of the contracted SLA threshold (configurable), providing advance warning to enable remediation before the penalty accrual trigger is reached.	SLA Threshold Early Warning Alerting
<b>FR-NMS-014</b>	The system shall automatically compute financial penalties for SLA breaches in accordance with the contract penalty formulae. The penalty computation report shall be generated at each monthly billing period and made available to NHAI and the relevant TSP.	Financial Penalty Auto-Computation
<b>FR-NMS-015</b>	Monthly SLA performance reports shall be automatically generated and made available to TSPs through the Contractor Portal. The report shall include, per device type per corridor: availability percentage, fault count, MTTR, MTBF, SLA threshold, breach amount, penalty amount, and cumulative YTD penalty.	Monthly SLA Report to TSP

#### 9.4.9.4. *Fault Management and Maintenance Ticketing*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-NMS-016</b>	Every device fault event automatically detected by the NMS shall generate a maintenance ticket containing: ticket ID (unique), device ID, fault type and description, KP location, detection timestamp, assigned TSP, target resolution time (based on contracted SLA per fault type), and ticket priority (Critical/Major/Minor mapped from fault severity).	Auto Ticket Creation
<b>FR-NMS-017</b>	Maintenance tickets shall be managed through a defined lifecycle: Open → Assigned (to TSP technician) → In Progress (technician on-site) → Resolved (technician marks fix done) → Verified (NHAI/LCCC supervisor confirms restoration) → Closed. Backwards transitions shall require supervisory approval.	Ticket Lifecycle States

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-NMS-018</b>	Field technicians shall update ticket status, add notes, attach photographs of fault and repair, and mark tickets as Resolved via the ATMS Mobile Application. All mobile updates shall sync to the central NMS in real time where connectivity exists, and on reconnection if offline.	Mobile Ticket Field Updates
<b>FR-NMS-019</b>	The system shall send automated reminder notifications to the TSP for tickets approaching their SLA resolution deadline: first alert at 80% of elapsed SLA time, second alert at 100% (SLA breach). Breach notifications shall also be sent to the NHAI contract manager.	Ticket SLA Reminders
<b>FR-NMS-020</b>	The system shall provide a preventive maintenance scheduling module: TSPs shall log scheduled maintenance visits (device ID, date/time window, maintenance type, technician name). The system shall automatically suppress SLA fault timers for devices covered by a pre-notified maintenance window during the notified period.	Preventive Maintenance Scheduling
<b>FR-NMS-021</b>	The Contractor Portal shall enable TSP users to: view SLA performance metrics for their contract scope, see all open/in-progress maintenance tickets, submit maintenance completion evidence (photographs, technician notes, parts used), view penalty computations, and download monthly SLA reports.	TSP Contractor Portal

## 9.5. SECTION B — ADDITIONAL SOFTWARE MODULES

<div><div>10</div><div>Open Source GIS &amp; Mapping (Extended)</div></div> <div><div>FR-GIS</div><ul style="list-style-type: none"><li>• PM Gati Shakti GIS integration</li><li>• Custom admin layers (blackspots, geofences)</li><li>• Road network + admin boundary data</li><li>• Multi-provider map (OSM/Google/Bing/ESRI)</li><li>• Route condition monitoring (Green/Amber/Red)</li><li>• Offline cached base map (weekly refresh)</li></ul></div>	<div><div>11</div><div>Data Management, Analytics &amp; Intelligence</div></div> <div><div>FR-DAT</div><ul style="list-style-type: none"><li>• Bronze/Silver/Gold 3-zone data lake</li><li>• Congestion prediction (1hr+4hr, ≥80% accuracy)</li><li>• Incident risk prediction model</li><li>• Predictive device maintenance model</li><li>• Weather-incident correlation (quarterly update)</li><li>• All AI outputs labelled 'AI Estimate'</li></ul></div>	<div><div>12</div><div>Platform Security &amp; Cybersecurity</div></div> <div><div>FR-SEC</div><ul style="list-style-type: none"><li>• Zero Trust Architecture (ZTA)</li><li>• SIEM: 200+ MITRE ATT&amp;CK rules + UEBA</li><li>• PAM: JIT privileged access + session record</li><li>• AES-256 at rest   TLS 1.3 in transit</li><li>• Annual CERT-In empanelled VAPT</li><li>• SBOM per deployment   ISO 27001:2022</li></ul></div>	<div><div>13</div><div>SLA Monitoring &amp; Asset Lifecycle (Extended)</div></div> <div><div>FR-SLA</div><ul style="list-style-type: none"><li>• SLA tier config: Standard/Enhanced/Critical</li><li>• SLA calendar view (90-day RAG history)</li><li>• Spare parts inventory + low-stock alerts</li><li>• Vendor device SLA from NMS telemetry</li><li>• Monthly penalty auto-report to TSP portal</li><li>• All vendor-sourced data attributed clearly</li></ul></div>	<div><div>14</div><div>Meteorological &amp; Environmental Monitoring</div></div> <div><div>FR-WTHR</div><ul style="list-style-type: none"><li>• 9-parameter AWS ingestion (5-min default)</li><li>• IMD forecast fusion — measured vs. forecast</li><li>• Configurable thresholds (visibility/wind/ice)</li><li>• Auto VMS advisory request to vendor VASD</li><li>• Weather-VMS audit chain (immutable log)</li><li>• 15-year AWS data retention in data lake</li></ul></div>
<div><div>15</div><div>Mobile Application &amp; Field Interface</div></div> <div><div>FR-MOB</div><ul style="list-style-type: none"><li>• React Native iOS (v16+) + Android (v12+)</li><li>• Offline-first + auto-sync on reconnection</li><li>• Maintenance ticket management &amp; photo capture</li><li>• Patrol incident reporting + GPS nav to scene</li><li>• AIS-140 GPS location pub to GIS every 30s</li><li>• Push: incidents, watch-list hits, broadcasts</li></ul></div>	<div><div>16</div><div>Alarm Display &amp; Management</div></div> <div><div>FR-ALM</div><ul style="list-style-type: none"><li>• Kafka-backed alarm bus (persistent store)</li><li>• Priority engine: type+location+SLA impact</li><li>• Alarm correlation (5-min/500m — anti-flood)</li><li>• Sources: ATMS-native + all vendor feeds</li><li>• Operator: Ack / Assign / Suppress / Close</li><li>• 5-year WORM alarm audit store</li></ul></div>	<div><div>17</div><div>Traffic Data to Road Users</div></div> <div><div>FR-PUB</div><ul style="list-style-type: none"><li>• Public PWA + iOS/Android (no login required)</li><li>• Traffic/incident/weather/VMS from ATMS feeds</li><li>• Opt-in corridor push notifications</li><li>• Separate read-only public API gateway (CDN)</li><li>• Rajmarg Yatra + NHAI App (MoRTH open data)</li><li>• Event marker detail: type/severity/ETA/advice</li></ul></div>	<div><div>18</div><div>Multi-Source Data Fusion &amp; Intelligence</div></div> <div><div>FR-SRC</div><ul style="list-style-type: none"><li>• Twitter/X + Facebook + RSS NLP ingestion</li><li>• NLP: incident type, location, severity extract</li><li>• Cross-source correlation engine (15-min/2km)</li><li>• Auto-SOP trigger at configurable confidence</li><li>• Multi-agency intelligence push notifications</li><li>• Cross-domain fusion: ITS+weather+enforcement</li></ul></div>	

Figure 21:Nine (9) Additional Modules

### 9.5.1. Module 10 — Open-Source GIS & Mapping Platform (Extended Capabilities)



Req ID	Requirement Description	Sub-Module / Feature
<b>FR-GIS-001</b>	The GIS platform shall integrate with PM Gati Shakti GIS, sharing real-time traffic conditions (from vendor ATCC/VIDS feed), incident events, ATMS asset data, and road condition information in the PM Gati Shakti standard data format for national infrastructure planning.	PM Gati Shakti Integration
<b>FR-GIS-002</b>	Administrators shall be able to define and manage custom GIS layers: geofenced enforcement zones, accident blackspot polygons, restricted areas, infrastructure layers, and planned road works zones. Custom layers shall be version-controlled with activation/deactivation date tracking.	Custom Administrator GIS Layers
<b>FR-GIS-003</b>	The GIS database shall include comprehensive road network data: national highways, state highways, city arterial roads, and urban streets with road name, classification, lane count, speed limits, and directionality. Administrative boundary data shall include state, district, sub-district, and town boundaries. All data shall be kept current through quarterly automated updates.	Road Network & Admin Boundaries
<b>FR-GIS-004</b>	The GIS platform shall display road condition monitoring on the map using green/amber/red corridor markings derived from: ATMS-managed sensor data, weather station readings, and available online road condition data sources. Route condition shall be updated every 15 minutes.	Route Condition Monitoring
<b>FR-GIS-005</b>	The GIS platform shall support integration with standard commercial and open map tile services (Google Maps, Bing Maps, ESRI ArcGIS, OpenStreetMap etc.). Map service provider shall be selectable by authorised administrators. The offline cached base map shall cover all ATMS project corridors at a minimum of 1:50,000 scale resolution and be refreshed weekly.	Multi-Provider Map Engine

### 9.5.2. Module 11 — Data Management, Analytics & Intelligence Platform (DMP)

#### 9.5.2.1. Data Storage and Lifecycle

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAT-001</b>	The system shall enforce minimum data retention periods for 10 years for following categories:	Data Retention Schedule



Req ID	Requirement Description	Sub-Module / Feature
	<ol style="list-style-type: none"> <li>1. TMCS/CCTV event metadata</li> <li>2. ANPR records and vehicle passage data</li> <li>3. Incident records</li> <li>4. Enforcement records and e-challan data</li> <li>5. Weather data</li> <li>6. Audit logs (permanent/indefinite);</li> <li>7. Call recordings linked to incidents (10 years minimum).</li> </ol>	
<b>FR-DAT-002</b>	The national data lake shall be hosted on-premise at Data Centre and DR on MEITY-empanelled cloud infrastructure. Data replication lag shall not exceed 30 seconds. No personal data of Indian citizens shall be stored outside India (data localisation). No data shall be stored on Cloud.	National Data Lake Architecture
<b>FR-DAT-003</b>	The system shall maintain data lineage records for every data object in the data lake: source system, ingestion timestamp, schema version, all transformation steps applied, and consuming applications. Data lineage shall be queryable by authorised Data Analysts via the ad-hoc query builder.	Data Lineage

#### 9.5.2.2. *AI and Predictive Analytics*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-DAT-004</b>	The system shall provide a traffic congestion prediction model computing 1-hour and 4-hour ahead congestion forecasts for each corridor segment, updated every 15 minutes. The model shall achieve minimum 80% accuracy (% of predictions within one congestion band of actual, validated on a rolling 3-month basis). Predicted congestion shall be displayed on the GIS map with 'AI Estimate' labels.	Congestion Prediction Model
<b>FR-DAT-005</b>	The system shall provide an incident risk prediction model identifying road segments and time periods with elevated incident probability, based on: historical incident data, weather conditions, traffic volumes (from vendor ATCC/VIDS feed), time of day, day of week, and special events. Risk predictions shall be presented to LCCC/RCCC supervisors as advisory heat maps.	Incident Risk Prediction Model
<b>FR-DAT-006</b>	The system shall provide a predictive device maintenance model identifying field devices with elevated failure probability within the next 30	Predictive Device Maintenance

Req ID	Requirement Description	Sub-Module / Feature
	days, based on: device age, fault history frequency, firmware version, MTBF statistics for the device model, and environmental operating data. Predictions shall surface in the NMS as preventive maintenance recommendations.	
<b>FR-DAT-007</b>	All AI/ML model predictions shall be clearly labelled as 'AI Estimate' in all dashboards and reports. Each prediction shall be accompanied by a confidence score and a brief explanation of the primary driving factor. Predictions shall not be presented as definitive operational facts.	AI Prediction Transparency & Explainability
<b>FR-DAT-008</b>	AI model performance shall be evaluated automatically on a monthly basis against actual outcomes. Model accuracy metrics (precision, recall, F1 score, MAPE for regression) shall be published to the System Administration dashboard. Models shall be flagged for retraining if accuracy falls below configured thresholds.	Model Performance Monitoring
<b>FR-DAT-009</b>	The system shall provide a weather-incident correlation analysis: using historical weather events correlated with historical incident records, the system shall identify weather types and thresholds most associated with incidents on each corridor, published as a corridor-specific risk matrix updated quarterly.	Weather-Incident Correlation Analysis
<b>FR-DAT-010</b>	The system shall provide a crowd-sourced big data repository: historical traffic data at road-segment level including ITS equipment data, crowd-sourced inputs (social media, Rajmarg Yatra, NHAI App), weather conditions, construction activity records, regulatory measures, and all incident records. The traffic, enforcement and incident data shall be segregated by corridor, vehicle class, vehicle type, fleet details if available. The repository shall support policy and planning decision support for transport planners and government authorities.	Crowd-Sourced Big Data Repository
<b>FR-DAT-011</b>	The analytics platform shall support a minimum set of visualisation types: bar charts, line charts, stacked area charts, pie/donut charts, heat maps, scatter plots, GIS choropleth maps, and Gantt charts (for SOP and maintenance planning). Custom visualisations shall be embeddable in custom reports.	Visualisation Library

### 9.5.3. Module 12 — Platform Security & Cybersecurity Architecture

#### 9.5.3.1. Access Control and Network Security

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SEC-001</b>	The system shall implement a Zero Trust Architecture (ZTA): no network location is implicitly trusted; every access request — regardless of network origin (internal LAN, VPN, public internet) — shall be validated against the IAM policy in real time. ZTA principles shall apply to all API connections including connections to Existing Field Platform Vendor systems.	Zero Trust Architecture
<b>FR-SEC-002</b>	The system shall implement network micro-segmentation to isolate NCCC, RCCC, LCCC, API gateway, data lake, SIEM, and administration network zones. Lateral movement between zones shall be prevented by default; all inter-zone traffic shall be validated and logged.	Network Micro-Segmentation
<b>FR-SEC-003</b>	The system shall implement Privileged Access Management (PAM) for all administrator accounts: all privileged sessions shall be recorded end-to-end (keystrokes and screen), just-in-time (JIT) privileged access shall be enforced (no standing privileged accounts except break-glass), and privileged session recordings shall be stored in an access-controlled, immutable repository.	Privileged Access Management (PAM)

#### 9.5.3.2. *Data Encryption and Integrity*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SEC-004</b>	All data at rest in the data lake, operational databases, call recording storage, and archive storage shall be encrypted using AES-256. All data in transit between system components, between tiers, to external systems (including vendor API feeds), and to end-user browsers shall be encrypted using TLS 1.3 minimum. TLS 1.0 and TLS 1.1 shall be explicitly disabled.	Encryption — At Rest & In Transit
<b>FR-SEC-005</b>	Encryption keys shall be managed using a MEITY-approved Key Management Service (KMS) with: automatic key rotation at intervals not exceeding 12 months, separation of duties (key generation, key use, and key deletion by different roles), hardware security module (HSM) backing, and key usage audit logging.	Key Management Service
<b>FR-SEC-006</b>	All enforcement evidence files (images, video clips), call recordings, and audit log archives shall be digitally signed with a tamper-evident hash at the time of creation. Any post-creation modification shall invalidate the	Evidence & Log Integrity Signing

Req ID	Requirement Description	Sub-Module / Feature
	signature and generate an immediate security alert to the SIEM and System Administrator.	

### 9.5.3.3. *Threat Detection, Monitoring, and Incident Response*

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SEC-007</b>	The system shall deploy a SIEM (Security Information and Event Management) platform collecting security events from all system components: application servers, databases, API gateway, network devices, endpoint agents (LCCC workstations). The SIEM shall apply correlation rules to detect: brute force attempts, privilege escalation, unusual data volumes, geographic anomalies, and lateral movement.	SIEM Deployment & Correlation
<b>FR-SEC-008</b>	The SIEM shall implement behavioural analytics (UEBA — User and Entity Behaviour Analytics) to detect: unusual login times, bulk data downloads, access from new geographic locations, access to resources outside normal patterns, and after-hours privileged access. Anomalies shall generate security alerts graded by risk score.	UEBA Behavioural Analytics
<b>FR-SEC-009</b>	Critical cybersecurity incidents shall be reported to CERT-In within 6 hours as required by CERT-In Directions 2022. An internal incident response playbook shall be maintained, tested annually, and available to the System Administrator from the ATMS security management console.	CERT-In Reporting & IR Playbook
<b>FR-SEC-010</b>	The system shall perform automated vulnerability scanning on all components at least monthly using a CERT-In empanelled scanning tool. Critical/High CVEs shall be patched within 72 hours of patch availability. Medium CVEs shall be patched within 30 days. Patch compliance status shall be published on the System Administration dashboard.	Vulnerability Scanning & Patch Management
<b>FR-SEC-011</b>	The system shall maintain a tamper-proof, immutable security audit log collecting all security events: authentications (success/failure), privilege changes, configuration changes, data exports, API calls, and access-denied events. The log shall not be modifiable or deletable by any user including system administrators. Log files shall be replicated to an offline air-gapped archive quarterly.	Immutable Security Audit Log
<b>FR-SEC-012</b>	Annual Vulnerability Assessment and Penetration Testing (VAPT) shall be conducted by a CERT-In empanelled firm. VAPT findings shall be	Annual VAPT

Req ID	Requirement Description	Sub-Module / Feature
	remediated within 90 days for Critical/High findings and 180 days for Medium findings. VAPT reports shall be submitted to NHAI/IHMCL.	
<b>FR-SEC-013</b>	The system shall register with NCIIPC as a Critical Information Infrastructure (CII) operator. A Secure Software Development Lifecycle (SSDLC) shall be maintained, including: static code analysis (SAST), dependency vulnerability scanning (SCA), and annual code review. Application hardening shall comply with OWASP Top 10 standards.	NCIIPC / CII & Secure SDLC
<b>FR-SEC-014</b>	The system shall maintain an up-to-date Software Bill of Materials (SBOM) for all system components, including: application code, dependencies, operating system packages, and container base images. The SBOM shall be scanned against known vulnerability databases automatically on each deployment.	Software Bill of Materials (SBOM)

#### 9.5.4. Module 13 — SLA Monitoring & Asset Lifecycle Management (Extended)

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SLA-001</b>	SLA computation for VIDES/ANPR/VMS/Sensors device availability shall use structured health telemetry received from the Existing Field Platform Vendor's NMS. The ATMS SLA engine shall compute availability based on uptime data shared by the vendor, clearly attributing the data source in the penalty computation report.	Vendor Device SLA Computation
<b>FR-SLA-002</b>	The SLA management module shall support configurable SLA tiers: Standard (>95% availability), Enhanced (>98%), and Critical (>99.5%), assignable per device type per corridor. SLA breach triggers and penalty rates shall be defined per tier per contract.	Configurable SLA Tiers
<b>FR-SLA-003</b>	The system shall provide an SLA compliance calendar view showing: daily availability scores per device type per corridor for the trailing 90 days, with breach days highlighted in red, warning days in amber, and compliant days in green.	SLA Calendar View
<b>FR-SLA-004</b>	The spare parts inventory sub-module shall enable TSPs to log spare parts stock at depot level (item name, quantity, device types applicable,	Spare Parts Inventory

Req ID	Requirement Description	Sub-Module / Feature
	last replenishment date). Automated low-stock alerts shall be generated when stock falls below a configurable minimum quantity.	

#### 9.5.5. Module 14 — Meteorological & Environmental Monitoring Module

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-WTHR-001</b>	The system shall ingest sensor readings from all roadside Automatic Weather Stations (AWS) at configurable intervals (default: 5 minutes) including: air temperature, road surface temperature, relative humidity, dew point, wind speed (instantaneous and 10-minute average), wind direction, precipitation type and intensity, road surface condition (dry, wet, icy, flooded, chemically wet), and visibility (in metres).	AWS Multi-Parameter Ingestion
<b>FR-WTHR-002</b>	The GIS map shall display current weather conditions at each AWS location using colour-coded overlay icons, updated at each data ingestion cycle. Icons shall change colour when any threshold is exceeded. The operator shall be able to click any AWS icon to view the full current parameter set and a 24-hour trend chart.	Weather GIS Display
<b>FR-WTHR-003</b>	The system shall generate weather alerts when any sensor reading exceeds predefined thresholds (configurable per corridor): visibility < 200 m (dense fog), road surface condition = icy, road surface condition = flooded, wind speed > 60 km/h, rainfall rate > 20 mm/hr, air temperature < 0°C with wet road surface (black ice risk). All threshold values shall be configurable by System Administrators.	Configurable Weather Threshold Alerts
<b>FR-WTHR-004</b>	Weather alerts shall automatically dispatch advisory message requests to the Existing Field Platform Vendor's VMS system for speed limit reduction advisories to the pre-configured safe speed for the triggering condition. This shall occur without operator intervention, subject to supervisor override capability. All automated requests shall be logged.	Automated VMS Advisory Request on Weather
<b>FR-WTHR-005</b>	Every VMS advisory request triggered by a weather event shall be logged in the ATMS audit trail with: triggering AWS ID, parameter breached, measured value, threshold, ATMS advisory request timestamp, vendor VMS system acknowledgement timestamp (if bidirectional interface is available), and sign ID. This chain shall provide a full audit trail from weather condition to VMS advisory.	Weather-to-VMS Advisory Audit Chain

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-WTHR-006</b>	IMD forecast data (received from IMD API integration) shall be fused with real-time AWS sensor data and displayed in the GUI. Measured conditions and forecast conditions shall be visually distinguished. A 24-hour forecast per corridor shall be displayed on the weather monitoring dashboard.	IMD Forecast Fusion
<b>FR-WTHR-007</b>	The system shall provide weather-incident correlation analysis: using at least 3 years of historical weather events correlated with historical incident records, the system shall identify weather types and threshold combinations most associated with incidents on each corridor type. Results shall be published as a corridor-specific seasonal risk matrix, updated quarterly.	Weather-Incident Correlation
<b>FR-WTHR-008</b>	All raw weather data from roadside AWS stations shall be retained in the national data lake for a minimum of 10 years. AWS data shall be accessible via API for external research and policy-making by authorised entities.	Weather Data 10-Year Retention
<b>FR-WTHR-009</b>	The weather monitoring dashboard shall display: current conditions at all AWS per corridor (tabular + GIS), active weather alerts, list of VMS advisory requests triggered in the last 24 hours, 24-hour trend chart per AWS parameter, and an upcoming 24-hour weather forecast.	Weather Monitoring Dashboard

#### 9.5.6. Module 15 — Mobile Application & Field Operator Interface

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-MOB-001</b>	The system shall provide a native mobile application for field maintenance staff and highway patrol officers, available for iOS (v16+) and Android (v12+). The app shall use the same MFA-based authentication as the desktop interface, with biometric unlock (fingerprint / Face ID) available after initial MFA login.	Mobile App Platform & Authentication
<b>FR-MOB-002</b>	Field maintenance technicians shall be able to: view all maintenance tickets assigned to them, filter by corridor/device type/priority, update ticket status through the lifecycle (In Progress → Resolved), add free-text notes and annotated photographs, record parts used, and capture technician sign-off with digital signature.	Maintenance Ticket Field Management



Req ID	Requirement Description	Sub-Module / Feature
<b>FR-MOB-003</b>	Highway patrol officers shall be able to: report incidents by selecting incident type and severity on a map, capture and attach photographs and video clips, add description notes, and receive incident assignments from the LCCC. The nearest registered CCTV camera (from vendor TMCS registry) shall be auto-identified and displayed for the reporting officer.	Patrol Incident Reporting
<b>FR-MOB-004</b>	The mobile app shall support GPS-based navigation to the location of an assigned incident or device fault, integrating with device maps (Google Maps / OpenStreetMap). Turn-by-turn directions shall be available for the final approach to the incident or device location.	GPS Navigation to Incident/Device
<b>FR-MOB-005</b>	The mobile app shall support full offline operation: all assigned ticket data and incident assignments shall be cached locally. All offline actions (status updates, notes, photographs, new patrol reports) shall be queued locally and synced to the central system automatically upon connectivity restoration, in correct sequence.	Offline Operation & Auto-Sync
<b>FR-MOB-006</b>	The mobile app shall receive and display push notifications for: new incident assignments from LCCC, watch-list vehicle detections near the officer's GPS location (watch-list data sourced from vendor ANPR platform), urgent broadcast messages from LCCC/RCCC supervisors, and ticket SLA deadline alerts. Notifications shall display even when the app is in background mode.	Push Notifications — All Event Types
<b>FR-MOB-007</b>	The mobile app shall provide a live feed view of up to 2 CCTV camera streams simultaneously for field supervisors. Stream tokens shall be received from the vendor TMCS platform through the ATMS API gateway. Stream quality shall auto-adjust based on available mobile data bandwidth.	Mobile CCTV Stream View
<b>FR-MOB-008</b>	The mobile app shall enable patrol officers to update their vehicle location (AIS-140/GNSS) in real time to the ATMS platform, making them visible on the LCCC/RCCC/NCCC GIS maps as patrol vehicle icons.	Patrol Vehicle Live Location Update
<b>FR-MOB-009</b>	The mobile app shall provide access to the Stakeholder Contacts Directory (Module D), enabling field staff to initiate calls to ambulance, police, maintenance teams, and NHAI officials directly from the app with one-tap dialling.	Mobile Contacts Directory & Dialling

#### 9.5.7. Module 16 — Alarm Display & Management Module

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-ALM-001</b>	The system shall provide centralised, real-time alarm presentation across all operator workstations: visual alerts (configurable pop-up notifications, colour-coded status indicators, dashboard area highlights) and audible alerts (configurable tones or synthesised spoken announcements per alarm category). Alert tone profiles shall be configurable per workstation.	Visual & Audible Alarm Notification
<b>FR-ALM-002</b>	The system shall support simultaneous handling and display of multiple alarms across multiple operator workstations without performance degradation or alarm queue overflow. The alarm management subsystem shall maintain full functionality during peak concurrent alarms from all corridors and all device types in the regional scope.	Multi-Alarm Multi-Workstation Handling
<b>FR-ALM-003</b>	Alarms shall be generated from both ATMS-native sources (device health, weather thresholds, SLA breaches, security events, system health) AND from structured alarm events received from the Existing Field Platform Vendor's systems (VIDES detection events, ANPR watch-list hits, VMS device faults, enforcement module alerts). The source system shall be clearly attributed on each alarm.	Multi-Source Alarm Ingestion
<b>FR-ALM-004</b>	The system shall automatically prioritise alarms using a configurable priority engine based on: alarm type, geographic location, associated device type, incident severity, SLA impact, and time elapsed since alarm generation. The highest-priority alarms shall be displayed first in the queue, highlighted in red, and presented in a separate 'Critical Alarms' panel.	Automatic Alarm Prioritisation
<b>FR-ALM-005</b>	Operators shall be able to acknowledge (with mandatory operator note), assign (to self or another operator), suppress with time-limit and mandatory reason (e.g., 'Under maintenance — suppressed for 2 hours'), and close alarms from the alarm display panel. All alarm actions shall be logged in the audit trail with timestamp, user ID, action, and notes.	Alarm Action Workflow & Audit
<b>FR-ALM-006</b>	The system shall display persistent critical condition warning indicators for: high congestion exceeding configurable threshold (e.g., >30 km on a single corridor), active accident-prone zone incidents, device availability below SLA threshold, and weather alert in effect. These indicators shall remain visible on the GIS map and the dashboard header until the condition is fully resolved or manually dismissed by an authorised supervisor.	Critical Condition Persistent Indicators

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-ALM-007</b>	The system shall implement alarm correlation: multiple alarms from the same device/location within a configurable time window shall be grouped into a single correlated alarm event to prevent alarm flooding. The correlation window and grouping rules shall be configurable by System Administrators.	Alarm Correlation & Grouping
<b>FR-ALM-008</b>	The alarm management module shall provide alarm analytics dashboards: alarm volume by type, corridor, time of day, and day of week; average acknowledge time; suppression frequency by alarm type; and repeat alarm frequency (same device recurring fault). Alarm analytics shall be available at LCCC, RCCC, and NCCC levels.	Alarm Analytics Dashboard

#### 9.5.8. Module 17 — Traffic Data Dissemination to Road Users

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-PUB-001</b>	The system shall provide road, traffic, and related information to road users through a graphical interface accessible via a public web application (mobile-responsive, no app install required) and a mobile application (iOS and Android). No registration or login shall be required for general traffic information access. The interface shall support English and Hindi.	Public Road User Web & Mobile App
<b>FR-PUB-002</b>	The road user interface shall present a consolidated, map-based view of: real-time traffic status (colour-coded congestion from vendor ATCC/VIDES feed), active incidents (from ATMS incident engine), weather conditions (from ATMS weather module), VMS messages (current message from vendor VMS platform), toll plaza status, and symbolic landmarks along national highways.	Consolidated Traffic Map View
<b>FR-PUB-003</b>	The map interface shall cover the complete national highway network and support smooth zoom and pan. Upon selection of a specific location or road segment, the interface shall display: real time traffic conditions (colour-coded congestion), estimated travel time between user-selected origin and destination (based on current speed data) based on traffic congestion, event information (accidents, construction, special events), and traffic regulations (road closures, diversions, speed restrictions).	Map Detail & Travel Time Estimation

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-PUB-004</b>	When a user selects an event marker, the application shall display detailed event information: location (highway name + KP), incident/event type, severity level, expected clearance time, NHAI advisory instructions, and nearest helpline contact (1033).	Event Marker Detail Panel
<b>FR-PUB-005</b>	The road user app shall allow users to opt in to route-specific push notifications for: incidents on their frequently travelled corridors, adverse weather alerts, planned road works, and emergency diversions. Notification frequency and types shall be configurable per user.	Personalised Push Notifications
<b>FR-PUB-006</b>	The road user app shall display the location and contact details of key highway services near the user's current location or selected corridor: petrol pumps, rest areas, hospitals, police stations, emergency lay-bys, and toll plazas.	Highway Services Nearby
<b>FR-PUB-007</b>	The system shall integrate with Rajmarg Yatra and the NHAI Mobile App for geo-tagged broadcast of traffic advisories and incident notifications. Data exchange format shall conform to MoRTH open data standards to allow future integration with any Government-designated road user information platform.	Rajmarg & NHAI App Integration

#### 9.5.9. Module 18 — Multi-Source Data Fusion & Intelligence Summarization

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SRC-001</b>	The system shall aggregate intelligence inputs from: ATMS-managed sensors and ECBs (direct), structured event feeds from Existing Field Platform Vendor systems (TMCS, Radar, VIDES, ANPR, VASD etc.), social media platforms (Twitter/X, Facebook, configurable RSS/news feeds), 1033/Rajmarg Yatra/NHAI App crowd reports, ITS equipment telemetry (from vendor ATCC/VIDS feed), and authorised third-party data sources. Aggregated inputs shall be correlated in real time to generate actionable alerts for operator response.	Multi-Source Intelligence Aggregation

Req ID	Requirement Description	Sub-Module / Feature
<b>FR-SRC-002</b>	The intelligence dashboard shall extract and display relevant messages, alerts, and data from all connected sources in a unified, real-time operational intelligence feed. Operators and supervisors across NCCC, RCCC, and LCCC tiers shall be able to access the dashboard, with data scoped to their tier and jurisdiction.	Intelligence Dashboard Feed
<b>FR-SRC-003</b>	The system shall correlate social media posts and crowd reports with structured events from vendor platforms and ATMS incident records. Correlation shall use: geo-location proximity (< 2 km radius), time proximity (< 15 minutes), and keyword/semantic matching for incident type. Auto-correlation matches shall be presented to the operator for confirmation.	Cross-Source Correlation Engine
<b>FR-SRC-004</b>	The system shall automatically recommend or initiate the appropriate SOP based on predefined correlation rules when multiple intelligence sources confirm an incident. Rule priority, confidence threshold (minimum correlation score to trigger auto-SOP), and affected SOP templates shall be configurable by authorised administrators.	Auto-SOP from Intelligence Fusion
<b>FR-SRC-005</b>	The system shall identify critical or high-priority intelligence based on configurable rules or analytics, and link it to an existing incident or automatically trigger initiation of a new SOP workflow. Priority identification thresholds, linkage rules, and trigger conditions shall be configurable by authorised administrators without coding.	Priority Intelligence & SOP Trigger
<b>FR-SRC-006</b>	The system shall provide real-time push notifications to multiple agencies based on aggregated intelligence. Notifications shall be configurable by: target agency, event type, minimum confidence threshold, minimum severity, and geographic scope.	Multi-Agency Intelligence Push Notifications
<b>FR-SRC-007</b>	Social media data ingested by the system shall be processed through a natural language processing (NLP) analytics engine to: extract incident type, location (when mentioned), severity indication, and road name. Processed signals shall be scored for operational relevance before surfacing in the intelligence dashboard.	NLP Social Media Processing
<b>FR-SRC-008</b>	The system shall provide cross-domain data fusion combining: ITS sensor data (from vendor ATCC/VIDS/ANPR/RADAR/VASD feed), enforcement records (from vendor e-Challan feed), weather data (ATMS AWS + IMD), crowd-sourced inputs, and incident history. Fused intelligence shall	Cross-Domain Data Fusion for Planning

Req ID	Requirement Description	Sub-Module / Feature
	support both operational decision-making and long-term policy and infrastructure planning.	

#### 9.5.10. Performance and Scale Targets

<b>Total simultaneous field devices (national)</b>	≥ 100,000
<b>Vehicle passage records processed per day</b>	≥ 10 million
<b>Event processing throughput (NCCC tier)</b>	≥ 100,000 events/second sustained
<b>Data ingestion latency (field device to data lake)</b>	≤ 5 seconds
<b>VIDES incident event to ATMS incident record</b>	≤ 5 seconds
<b>Connectivity loss autonomous LCCC operation</b>	168 hours minimum
<b>GUI response time for operator actions</b>	≤ 2 seconds (P95) under full load
<b>Live video stream token delivery (cross-tier)</b>	≤ 5 seconds from request
<b>API response time (external integrations)</b>	≤ 3 seconds (P95)
<b>System availability (NCCC/RCCC/LCCC)</b>	≥ 99.9% (monthly)
<b>Recovery Point Objective (critical data)</b>	2 hour
<b>Recovery Time Objective (full system restoration)</b>	4 hours
<b>Concurrent user sessions (all tiers combined)</b>	≥ 5,000

## 10. PROJECT IMPLEMENTATION TIMELINE – 12 MONTHS

The National ATMS ICCC Platform implementation is structured across a 12-month implementation period from Contract Award (T0) to System Go-Live and O&M Commencement (T0+12). The timeline is divided into four phases, with clear milestone gateways that must be formally accepted by IHMCL before the next phase commences.

### 10.1. Implementation Timeline Summary

Timeline in Months	Phase
<b>Phase 1 (T0 to T0+2)</b>	Project Initiation, Requirement Gathering & SRS approval
<b>Phase 2 (T0+2 to T0+8)</b>	Development, Integration, and LCCC Rollout
<b>Phase 3 (T0+9 to T0+12)</b>	Pilot Operations, Performance Testing, Security Audit, Go-Live
<b>Phase 4 (T0+12 to T0+120)</b>	(Wave 1: 150 LCCCs, Wave 2: 250+ LCCCs and Wave 3: 667 LCCs)
<b>O&amp;M Period</b>	T0+9 to T0+120 — 10 Years

### 10.2. Phase 1 – Project Initiation, Requirement Gathering & SRS approval (T0 to T0+1)

Wk	Activity	Deliverable	Responsible
W1–2	Project kick-off, team mobilisation, PMO establishment	Project Charter; Project Management Plan; Risk Register; ATMS Master Schedule	PM + IHMCL
W1–4	Detailed requirements review; SRS baseline and RTM finalisation	Baselined SRS v2.0; Requirements Traceability Matrix (RTM)	PM + Dev Lead

### 10.3. Phase 2 – Development, Integration, and LCCC Rollout (T0+2 to T0+8)

Month	Activity	Deliverable	Responsible
M5	All 18 ATMS Platform modules core engine development and unit testing complete (>90% pass rate)	Sprint release notes; unit test results	Dev Team
M5-6	AI predictive analytics model training: congestion prediction and incident risk models trained on historical corridor data	AI model performance benchmarks; minimum accuracy thresholds achieved	AI/Data Team



Month	Activity	Deliverable	Responsible
M6	All 19 government system integrations integration-tested	Integration test reports; API test certificates	Dev + Integration
M6	Integrated Audio Communication Engine: 1033/ECB integration, call recording, in-platform messaging tested end-to-end	Audio communication test report; call recording sample review	Dev + Test
M6–7	SOP engine: all standard SOPs configured; SOP simulation tests completed; Mobile app published to app stores	SOP library with test results; Mobile app release v1.0	Ops + Dev Team
M8	Performance testing, load test, failover test, DR simulation	Performance test report	Test Team

#### 10.4. Phase 3 – Pilot Operations, Performance Validation, Go-Live (T0+09 to T0+12)

Month	Activity	Deliverable	Responsible
M9	<b>User Acceptance Testing (UAT)</b> with IHMCL/NHAI nominated users across 1 NCC, 2 RCCs, 10 LCCCs	UAT test cases; UAT results; IHMCL/NHAI UAT sign-off	PM + IHMCL/NHAI
M9–10	Operator training Phase 1: NCCC operators, RCC operators, LCCC senior operators — all 18 module workflows covered	Training completion certificates; operator assessment results	Training Team
M10	Security audit: CERT-In empanelled VAPT; secure code review; application hardening verification against CIS Benchmarks and OWASP	VAPT report; code review report; hardening checklist; CERT-In submission	Security + External
M11	Annual DR test (full DC → DR failover simulation): RTO <2 hours; RPO <4 hour; IHMCL sign-off	DR test report; RTO/RPO validation; signed by IHMCL Technical Director	Infra + Security
M11–12	Defect remediation; final performance tuning; final security hardening; SBOM updated	Defect closure report; final hardening checklist; updated SBOM	Dev + Security
M12	<b>Go-LIVE:</b> System Acceptance Certificate (SAC) issued by IHMCL: platform accepted,	Signed SAC; O&M commencement certificate; Exit Plan accepted	PM + IHMCL

Month	Activity	Deliverable	Responsible
	O&M commenced; Transition and Exit Plan submitted		

**10.5. Phase 4 – Full Rollout, Integration Testing, UAT (Wave 1: 150 LCCCs, Wave 2: 250+ LCCCs and Wave 3: 667 LCCs) (T0+12 to T0+120)**

Month	Activity	Deliverable	Responsible
Year 1 to 3	Wave 1 LCCC deployment: 150 LCCCs (NCCC + 2 RCCCs + 150 LCCs) commissioned; VDIL vendor feeds active per corridor	LCCC SAT reports per site; Wave 1 Go-Live certificate	Field Team
Year 4 to 5	Wave 2 LCCC deployment: remaining 250+ LCCCs commissioned across all 5 zones; all 20 RCCCs connected to NCCC	Zone-wise SAT reports; Wave 2 deployment completion certificate; NCCC-RCCC-LCCC hierarchy functional test	Field + Infra
Year 5 to 10	Wave 3 LCCC deployment: remaining LCCCs commissioned connected to NCCC	Wave 3 deployment completion certificate	Field + Infra

## 10.6. 10-YEARs' COMPREHENSIVE OPERATIONS & MAINTENANCE FRAMEWORK

From the date of System Acceptance Certificate (Month 12 from Contract Award, defined as T+GO-LIVE), the System Integrator shall provide comprehensive Operations and Maintenance (O&M) services for a period of 10 years. The O&M framework encompasses three service categories: Corrective Maintenance, Preventive Maintenance, and Development-cum-Enhancement support.

### 10.6.1. Cloud Infrastructure Monitoring and Reliability Management

The IA shall be responsible for continuous monitoring and operational management of all cloud infrastructure components supporting the ATMS Platform:

- Compute environment monitoring: CPU, memory, container health, auto-scaling triggers
- Application service monitoring: microservice health, inter-service latency, error budgets
- Data pipeline monitoring: Kafka consumer lag, ETL job health, data lake ingestion rates
- Platform observability: distributed trace analysis, log anomaly detection, metric dashboards
- Capacity management: monthly capacity reports, proactive scaling recommendations
- Cost management: cloud cost optimization monitoring and quarterly reports to IHMCL
- Cloud service incident management: liaison with cloud service provider for infrastructure incidents
- Reliability engineering: SLO/SLA tracking for all platform services

**Note:** The cloud infrastructure for deployment of the NCCC software shall be provisioned by NHAI/IHMCL. However, monitoring and ensuring uptime of the deployed application shall be the sole responsibility of the SDA. The SDA shall promptly report any faults or incidents to the designated officials of NHAI/IHMCL

### 10.6.2. O&M Team Composition

The O&M team composition is as follows:

Location tier / Team	Yrs 2–3 (Full)	Yrs 4–7 (Adjusted)	Yrs 8–10 (Reduced)	Primary driver of change between periods
A — NCCC Platform Support	11	8	4	Platform stabilises
B — RCCC Application Support	5	5	4	Stable from Year 3; slight consolidation in Years 5–10 as platform matures
C — LCCC Field Technical Support	8	13	12	Scales with live corridor count (avg 135 → 540 → 667); matures — ratio improves
D — Programme Management & Quality	2	2	1	

Location tier / Team	Yrs 2–3 (Full)	Yrs 4–7 (Adjusted)	Yrs 8–10 (Reduced)	Primary driver of change between periods
<b>TOTAL FTEs</b>	<b>26</b>	<b>28</b>	<b>21</b>	

Role	Responsibility
Platform Systems Expert	Architecture-level troubleshooting, escalation, vendor coordination
Operations Experts (Change/Problem Resolution)	Root cause analysis, change management, service restoration
Operations Leads (Incident Resolution)	Incident management, escalation coordination, SLA monitoring
Operations Engineers (Monitoring/Alerts/Health)	24x7 monitoring, first-line response, ticket management, health checks
Operations Support Developers	Bug fixing, patch implementation, minor enhancements

### 10.6.3. O&M Service Levels

Fault Category	Definition	First Response SLA	Resolution SLA	Penalty for Breach
<b>P1 – Critical</b>	NCCC/RCCC platform down; >20% LCCCs offline; major cybersecurity incident	15 minutes	4 hours	0.5% contract value per hour
<b>P2 – High</b>	Single RCC down; >5% LCCCs offline; enforcement pipeline failure; GIS unavailable	30 minutes	8 hours	0.25% per 4-hour breach
<b>P3 – Medium</b>	Single LCCC down; AI engine degraded; integration fault; VMS control failure	2 hours	24 hours	0.1% per day breach
<b>P4 – Low</b>	Non-critical feature defect; cosmetic UI issue; report formatting error	4 hours	5 business days	Tracked; no financial penalty

<b>P5 Enhancement</b>	– New feature request; configuration change; data model extension	5 business days (estimation)	Per agreed enhancement schedule	Per agreed milestone
-----------------------	---	------------------------------	---------------------------------	----------------------

#### 10.6.4. Development-cum-Enhancement Support Team (DEST)

The System Integrator shall provide a dedicated Development-cum-Enhancement Support Team (DEST) throughout the 10-year O&M period. This team is responsible for all platform software enhancements, new integration development, AI model retraining, bug fixing, security patching, and technology refresh activities. The DEST shall be co-located at the NCCC (or as agreed with NHAI/IHMCL) for day-to-day work with remote work permitted for development activities. The vendor may deploy other engineers in remote mode at their own premises to meet the stringent timelines for the project, including: Frontend/ Backend/ Full Stack Developers, Mobile App Developers, Database Architect, Solution Architect, UI/UX Designer, Security Architect, Cloud/DevOps Engineer.

Role	Experience	Count	Responsibilities
<b>Project Manager</b>	Minimum 15 years (ITS / software / large-scale infra)	1 (Full-Time, On-Site)	<ul style="list-style-type: none"> <li>• Overall O&amp;M delivery accountability; NHAI/IHMCL primary interface</li> <li>• Monthly and quarterly performance review; SLA governance</li> <li>• Annual capacity planning and technology refresh planning</li> <li>• Enhancement roadmap management and prioritisation</li> <li>• Escalation management; vendor coordination; change control</li> </ul>
<b>Senior Developer</b>	Minimum 8 years (Java / Python / Cloud / AI-ML)	1 (Full-Time; On-Site / Remote as agreed)	<ul style="list-style-type: none"> <li>• Platform enhancement development: new features, integrations</li> <li>• AI/ML model retraining and performance optimisation</li> <li>• Critical bug investigation and root cause analysis</li> <li>• Security patch assessment and implementation</li> <li>• Code review; architecture guidance for Jr. Developer</li> </ul>

<b>Junior Developer</b>	Minimum 3 years (Java / Python / JavaScript)	1 (Full-Time; Remote with monthly on-site)	<ul style="list-style-type: none"> <li>• Feature development and bug fixing (P3/P4 defects)</li> <li>• UI/UX enhancements to Common GUI</li> <li>• API integration development for new government systems</li> <li>• Automated test script development and maintenance</li> <li>• Documentation maintenance (technical guides, release notes)</li> </ul>
<b>QA / Test Engineer</b>	Minimum 6 years (ATMS / web apps / automation testing)	1 (Full-Time; Remote with quarterly on-site)	<ul style="list-style-type: none"> <li>• Test planning and execution for all platform releases</li> <li>• Regression testing for all enhancements and patches</li> <li>• Performance and load testing for annual scaling upgrades</li> <li>• VAPT preparation and remediation verification</li> <li>• User acceptance testing coordination with NHAI/IHMCL</li> </ul>

**10.6.5. Annual O&M Activities Calendar**

Annual Activity	Q1	Q2	Q3	Q4	Frequency	Owner
Platform software version upgrade (major release)	✓			✓	Annual (Q1 + Q4)	Sr Dev + PM
Platform software patch release (minor/security)	✓	✓	✓	✓	Quarterly	Sr Dev + DEST
AI model retraining (congestion + incident risk)		✓		✓	Bi-Annual	Sr Dev + AI
Annual VAPT by CERT-In empanelled auditor			✓		Annual	Tester + Security
Third-party platform audit (ISO 27001, MEITY, NCIIPC)				✓	Annual	PM + External Auditor
Annual Disaster Recovery full test (DC→DR)				✓	Annual — Q4	Infra + PM

Annual Activity	Q1	Q2	Q3	Q4	Frequency	Owner
Quarterly SLA performance review and penalty computation	✓	✓	✓	✓	Quarterly	PM + IHMCL
Cybersecurity licence renewal (SIEM, EDR, PAM etc. tools)				✓	Annual	Security + PM
Firewall ruleset and IDS/IPS signature update	✓	✓	✓	✓	Quarterly	Security
Operator refresher training programme	✓				Annual (by 31 March)	Training + PM
New operator induction training	✓	✓	✓	✓	As needed	Training
Annual programme performance report to NHAI				✓	Annual	PM + NCC Ops
Technology refresh assessment				✓	Annual (Y3 onwards)	PM + Infra
Vendor support contract renewals				✓	Annual	PM
SBOM update and vulnerability scan	✓	✓	✓	✓	Each deployment	DevOps + Security



## 11. CYBERSECURITY FRAMEWORK OVERVIEW

The National ATMS ICCC Platform, as a Critical Information Infrastructure (CII) under the NCIIIPC framework, is subject to the most stringent cybersecurity obligations applicable to Indian government information systems. This volume defines all cybersecurity implementation requirements across two categories: One-Time (OT) activities performed during the 12-month implementation phase, and Annual (ANN) / Ongoing (CONT) activities performed throughout the 10-year O&M period.



Figure 22: Governance, Compliance & 10-Year Sustainability

### 11.1. Applicable Standards and Directives

1. CERT-In Directions on Information Security, April 2022 (mandatory reporting, logging, auditing)
2. NCIIIPC Guidelines for Protection of Critical Information Infrastructure
3. MeitY Cloud Security Guidelines (for MEITY-empanelled CSP usage)
4. ISO/IEC 27001:2022 – Information Security Management Systems
5. ISO/IEC 27017:2015 – Cloud Security Controls
6. NIST Special Publication 800-207 – Zero Trust Architecture
7. NIST SP 800-53 Rev. 5 – Security and Privacy Controls
8. OWASP Top 10 (Application Security)
9. OWASP ASVS 4.0 (Application Security Verification Standard)
10. PCI-DSS (where FASTag payment data is handled)
11. Digital Personal Data Protection Rules, 2025

### 11.2. SECURE CODE REVIEW & APPLICATION HARDENING

#### 11.2.1. Secure Software Development Lifecycle (SSDLC)

All software developed for the unified ATMS Platform shall follow a Secure Software Development Lifecycle (SSDLC) that integrates security practices at every phase of development, from requirements through design, coding, testing, deployment, and maintenance. Security is not a phase in the development process; it is embedded in every phase.

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-SSDLC-001</b>	The SDA shall implement a formal SSDLC policy governing all platform software development and enhancement activities, covering threat modelling, security design reviews, secure coding standards, code review, and security testing.	<b>One-Time</b>	All	OWASP ASVS 4.0
<b>FR-SSDLC-002</b>	Threat modelling using STRIDE methodology shall be performed for all new features and major enhancements before design finalisation. Threat model outputs shall be documented and addressed in the design.	<b>One-Time</b>	All	NIST 800-53
<b>FR-SSDLC-003</b>	All platform source code shall undergo automated Static Application Security Testing (SAST) using an approved SAST tool (e.g., Jenkins, SonarQube, Checkmarx, Veracode) as part of the CI/CD pipeline. No code with Critical or High severity SAST findings shall be merged to the main branch.	<b>OT/CONT</b>	All	OWASP / CERT-In
<b>FR-SSDLC-004</b>	All third-party libraries and open-source components used in the platform shall be inventoried in a Software Bill of Materials (SBOM). The SBOM shall be scanned against known vulnerability databases (NVD, CISA KEV) as part of every build.	<b>OT/CONT</b>	All	NIST 800-53 SA-15
<b>FR-SSDLC-005</b>	All third-party libraries with Critical (CVSS $\geq$ 9.0) or High (CVSS $\geq$ 7.0) CVEs shall be updated or mitigated within 72 hours and 14 days respectively. CERT-In shall be notified for Critical CVEs as required.	<b>Ongoing</b>	All	CERT-In Dir 2022
<b>FR-SSDLC-006</b>	Dynamic Application Security Testing (DAST) shall be performed against the full platform in the UAT/Staging environment before every major release and annually during O&M.	<b>OT/ANN</b>	All	OWASP Top 10
<b>FR-SSDLC-007</b>	Interactive Application Security Testing (IAST) shall be deployed in the UAT environment to provide real-time security feedback during functional testing.	<b>One-Time</b>	All	OWASP ASVS

<b>FR-SSDLC-008</b>	All platform web interfaces shall be tested against and remediated for the full OWASP Top 10 (2021) vulnerability classes before go-live and after every major release.	<b>OT/ANN</b>	All	OWASP Top 10
---------------------	---	---------------	-----	--------------

**11.2.2. Secure Code Review (One-Time and Annual)**

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-SCR-001</b>	A comprehensive manual secure code review of the complete ATMS Platform codebase shall be conducted by a CERT-In empanelled security organisation before go-live. The review shall cover: authentication and authorisation logic, cryptographic implementations, input validation and sanitisation, API security, session management, and data access controls.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-SCR-002</b>	The code review report shall categorise findings by severity (Critical, High, Medium, Low) and provide specific remediation guidance for each finding. All Critical and High findings shall be remediated before go-live.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-SCR-003</b>	A focused secure code review shall be performed annually during O&M by a CERT-In empanelled auditor, covering all code changes made in the preceding 12 months (enhancement and patch code).	<b>Annual</b>	All	CERT-In Dir 2022
<b>FR-SCR-004</b>	The internal development team shall conduct mandatory peer code reviews using a security-focused code review checklist for all code changes before merging. The checklist shall be maintained and updated annually.	<b>Ongoing</b>	All	OWASP Code Review
<b>FR-SCR-005</b>	Code review findings and remediation status shall be tracked in the platform's issue management system, with NHAI/IHMCL having read-only access to the security findings tracker.	<b>Ongoing</b>	All	ISO 27001 A.8

**11.2.3. Application Hardening**

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-HARD-001</b>	All platform operating system images (for cloud VMs and LCCC servers) shall be hardened using CIS Benchmarks (Level 1 minimum, Level 2 for production) before	<b>One-Time</b>	All	CIS Benchmarks

	deployment. Hardening configuration shall be managed through IaC and validated on each build.			
<b>FR-HARD-002</b>	All platform web servers (NGINX, Apache, or equivalent) shall be configured with TLS 1.3, HSTS with preload, X-Content-Type-Options, X-Frame-Options, Content Security Policy (CSP), and Referrer-Policy headers. The system may also utilize Content Delivery Network (CDNs) to provide Dynamic Content Acceleration and Edge Computing capabilities at LCCC/RCCC/Mobile App level, as required.	One-Time	All	OWASP Secure Headers
<b>FR-HARD-003</b>	All containerised workloads shall run with the least-privilege security context: non-root user, read-only root filesystem where possible, no privileged containers, and seccomp profiles applied.	One-Time	All	CIS Kubernetes Benchmark
<b>FR-HARD-004</b>	All Kubernetes cluster configurations shall comply with the CIS Kubernetes Benchmark (Level 1). RBAC shall be enforced for all cluster resources; no wildcard permissions shall be granted.	One-Time	All	CIS K8s Benchmark
<b>FR-HARD-005</b>	Database servers shall be hardened: only required ports open; no default credentials; database access only through application service accounts with minimum required privileges; audit logging enabled on all database instances.	One-Time	All	CIS Database Benchmark
<b>FR-HARD-006</b>	All default credentials, sample applications, and unnecessary services shall be removed from all platform components before deployment. A hardening verification checklist shall be completed and signed off for each environment.	One-Time	All	CIS Benchmarks
<b>FR-HARD-007</b>	Application hardening compliance shall be re-verified after every major infrastructure change and annually during O&M, with re-hardening performed where drift from the baseline is detected.	Annual	All	CIS Benchmarks
<b>FR-HARD-008</b>	Mobile applications (field operator app) shall be hardened per OWASP Mobile Security Testing Guide (MSTG) and tested against the OWASP Mobile Application Security Verification Standard (MASVS) before release.	OT/ANN	All	OWASP MSTG

<b>FR-HARD-009</b>	Consumer data protection and privacy will be maintained as per requirements of DPDP Act, especially for all driver and financial information obtained via SARATHI integration and FASTag related information.	<b>OT/Ongoing</b>	All	DPDP 25
--------------------	---	-------------------	-----	---------

### 11.3. SIEM DEPLOYMENT AND LOG MANAGEMENT

#### 11.3.1. SIEM Platform Requirements

A centralised Security Information and Event Management (SIEM) platform shall be deployed as part of the ATMS ICCC Platform implementation. The SIEM serves as the central nervous system of the platform's security monitoring capability, ingesting security events from all platform components, applying correlation rules and ML-based analytics, and generating actionable alerts for the Cybersecurity Operations Centre (CSOC).

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-SIEM-001</b>	A SIEM platform shall be deployed as part of the one-time implementation, capable of ingesting security events from all NCCC, RCCC, and LCCC platform components, cloud infrastructure, network devices, and endpoint agents.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-SIEM-002</b>	The SIEM shall support ingestion from the following source types at a minimum: OS syslogs (Linux/Windows), application logs (platform services), infrastructure audit logs (Opensource Grafana Loki/ Elastic ELK Stack or cloud provider Azure Monitor / AWS CloudTrail), network flow logs (NetFlow/IPFIX), firewall logs, IDS/IPS alerts, EDR telemetry, and authentication system logs.	<b>One-Time</b>	All	SIEM architecture
<b>FR-SIEM-003</b>	The SIEM platform shall be capable of ingesting a minimum of 10,000 events per second (EPS) at go-live, scaling to 100,000 EPS by Year 5 without platform replacement.	<b>One-Time</b>	NCCC	29 YoY Scaling
<b>FR-SIEM-004</b>	The SIEM shall provide a library of minimum 200 pre-built detection rules aligned with the MITRE ATT&CK framework, covering initial access, persistence, privilege escalation, lateral movement, exfiltration, and impact tactics.	<b>One-Time</b>	NCCC	MITRE ATT&CK
<b>FR-SIEM-005</b>	The SIEM shall provide ML-based User and Entity Behaviour Analytics (UEBA) to detect anomalous behaviour patterns indicating insider threats, compromised credentials, and lateral movement, supplementing rule-based detection.	<b>One-Time</b>	NCCC	NIST 800-53 SI-4

<b>FR-SIEM-006</b>	The SIEM shall generate automated alerts for all critical security events including: multiple failed logins (>5 in 5 minutes), privilege escalation, access outside business hours, large data downloads, new device on network, and policy violations.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-SIEM-007</b>	SIEM alert triage, investigation, and response shall be performed by the 24x7 CSOC team. SIEM workflows shall include automated playbooks for common alert types, reducing mean time to respond (MTTR) for P1 security incidents to under 15 minutes.	<b>Ongoing</b>	NCCC	ISO 27001 A.5.25
<b>FR-SIEM-008</b>	The SIEM shall generate automated CERT-In incident report drafts for critical cyber incidents (detected category), pre-populated with incident details, timestamps, affected systems, and initial assessment, to support mandatory 6-hour reporting.	<b>Ongoing</b>	NCCC	CERT-In Dir 2022
<b>FR-SIEM-009</b>	SIEM software licenses, threat intelligence feeds, and cloud connector licenses shall be renewed annually before expiry. License renewal shall be included in the annual O&M budget.	<b>Annual</b>	NCCC	34.3 Annual Calendar
<b>FR-SIEM-010</b>	Annual SIEM health assessment shall be performed to review detection rule effectiveness, tune false-positive rates, update MITRE ATT&CK coverage, and incorporate lessons learned from the preceding year's security incidents.	<b>Annual</b>	NCCC	ISO 27001 A.5.7

### 11.3.2. Log Management Requirements

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-LOG-001</b>	All platform components (application servers, databases, API gateway, authentication systems, network devices, cloud infrastructure) shall forward security-relevant logs to the centralised SIEM platform in real-time.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-LOG-002</b>	The following events shall be logged at a minimum for all platform components: login success and failure, logout, privilege escalation, configuration changes, API calls (request, response status, user identity), data access on sensitive records (enforcement evidence, ANPR records), and system errors.	<b>One-Time</b>	All	CERT-In Dir 2022

<b>FR-LOG-003</b>	Log entries shall contain the following fields at a minimum: timestamp (UTC, millisecond precision, NTP synchronised), source system identifier, log level, user identity (if applicable), source IP address, action performed, affected resource, and outcome (success/failure).	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-LOG-004</b>	All audit and security logs shall be stored in a tamper-evident, WORM-protected log store with a minimum retention period of 5 years, accessible for investigation within 15 minutes of an authorised request.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-LOG-005</b>	Log integrity shall be verified using cryptographic hashing (SHA-256 minimum) applied to each log batch. Hash values shall be stored separately from the logs in an independent immutable store.	<b>One-Time</b>	All	ISO 27001 A.8.15
<b>FR-LOG-006</b>	All LCCC edge nodes shall implement local log buffering for a minimum of 168 hours during WAN outage. Buffered logs shall be forwarded to the SIEM in chronological order upon WAN restoration, without loss.	<b>One-Time</b>	LCCC	5.4.3 Edge autonomy
<b>FR-LOG-007</b>	Log shipping from all components to the SIEM shall be encrypted using TLS 1.3 and authenticated. No plaintext log transmission shall be permitted.	<b>One-Time</b>	All	10.3 Encryption
<b>FR-LOG-008</b>	The log management platform shall provide a search and investigation interface enabling CSOC analysts to query across all log sources with full-text search, field-based filtering, and time-range queries, returning results within 30 seconds for queries spanning up to 90 days of data.	<b>One-Time</b>	NCCC	SIEM architecture

#### 11.4. ENDPOINT DETECTION AND RESPONSE (EDR)

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-EDR-001</b>	Enterprise-grade EDR software shall be deployed on all NCCC and RCCC platform servers, operator workstations, and administrative laptops during the one-time implementation phase.	<b>One-Time</b>	NCCC /RCCC	NCIIPC CII
<b>FR-EDR-002</b>	EDR agents shall be deployed on all LCCC edge servers (primary and standby) at each LCCC during the commissioning phase.	<b>One-Time</b>	LCCC	NCIIPC CII



<b>FR-EDR-003</b>	The EDR platform shall provide the following capabilities at minimum: real-time process monitoring, file integrity monitoring (FIM), network behaviour monitoring, memory protection, ransomware detection and rollback, and threat hunting capability.	<b>One-Time</b>	All	NIST 800-53 SI-3
<b>FR-EDR-004</b>	The EDR platform shall integrate with the centralised SIEM, forwarding all EDR alerts and telemetry to the SIEM for correlation with other security event sources.	<b>One-Time</b>	All	37.1 SIEM
<b>FR-EDR-005</b>	EDR policy shall prevent execution of unsigned binaries, restrict access to administrative tools (PowerShell, cmd, scripting engines) on production servers to authorised administrators only.	<b>One-Time</b>	All	NIST 800-53 CM-7
<b>FR-EDR-006</b>	EDR threat intelligence and detection signature updates shall be applied automatically at minimum every 4 hours, without requiring manual administrator intervention or server restart.	<b>Ongoing</b>	All	EDR vendor SLA
<b>FR-EDR-007</b>	EDR software licenses shall be renewed annually before expiry. Renewal shall include entitlement to the latest product version, updated threat intelligence feeds, and vendor technical support.	<b>Annual</b>	All	34.3 Annual Calendar
<b>FR-EDR-008</b>	Annual EDR health review shall be conducted to assess detection coverage, policy effectiveness, false-positive rates, and alignment with the current threat landscape.	<b>Annual</b>	All	ISO 27001 A.5.7

#### 11.5. Identity Access Management (IAM)

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-IAM-001</b>	The IAM solution supports authenticate, authorize, administrate and audit users, it can be integrated with AD/LDAP, etc.	<b>One-Time</b>		
<b>FR-IAM-002</b>	The IAM solution supports single sign-on/off, SAML 2, OIDC, etc. It supports service portal for the profile management.	<b>One-Time</b>		
<b>FR-IAM-003</b>	The IAM solution supports user & groups management, RBAC/ABAC, and centralized access control.	<b>Annual</b>		

<b>FR-IAM-004</b>	The IAM solution supports disablement/deletion of unused or expired accounts, entitlement exclusion (e.g., separation of duties)	<b>Annual</b>		
<b>FR-IAM-005</b>	The IAM solution should maintain summary of separation of users who are transferred, retired, or left the organization. It has a user lifecycle management facility.	<b>Annual</b>		
<b>FR-IAM-006</b>	The IAM solution supports storing passwords in encrypted format not in clear text, provides password expiry date, and has recommendations on password change as per defined policy.	<b>Annual</b>		

### 11.6. Privileged Access Management (PAM)

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-PAM-001</b>	The PAM solution supports 4A protocols i.e. authentication, auditing, accounting & authorization	<b>One-Time</b>		
<b>FR-PAM-002</b>	The PAM solution supports privileged Session Protocols - Terminal rdp, vnc, ssh, telnet etc.	<b>One-Time</b>		
<b>FR-PAM-003</b>	The PAM solution supports Unified Login and Authentication for resource; LDAP/AD authentication; RADIUS authentication; Single Sign-on (OpenID authentication, CAS authentication); SSO integration	<b>One-Time</b>		
<b>FR-PAM-004</b>	Isolation should be able to control the commands executed by authorized system users; Authorized system users' command execution is under control.	<b>Annual</b>		
<b>FR-PAM-005</b>	The PAM solution should support online session content auditing and historical session content auditing;	<b>Annual</b>		
<b>FR-PAM-006</b>	The PAM solution should have the following components: 1. Console 2. Workbench 3. Audit	<b>Annual</b>		
<b>FR-PAM-007</b>	The PAM solution should have option to create the ACL (Access command lists) to give more granular level authorization	<b>Annual</b>		

**11.6.1. Network Segmentation Design**

The platform network shall be segmented into security zones, with strictly controlled traffic flows between zones. The following zone model shall be implemented:

Network Zone	Hosts / Systems	Ingress From	Permitted To	Egress To
<b>DMZ (Public)</b>	API Gateway, WAF, Load Balancer, Developer Portal	Internet (filtered by WAF)		App Zone (HTTPS only)
<b>App Zone</b>	ICCC Core Engine, GIS Server, Notification Service, SOP Engine	DMZ (HTTPS), Operator Zone (HTTPS)		Data Zone, Integration Zone
<b>AI / GPU Zone</b>	ANPR Engine, VCA Engine, ML Training Cluster	App Zone (internal API only)		Data Zone
<b>Data Zone</b>	PostgreSQL, MySQL, MongoDB, InfluxDB, ClickHouse, Data Lake, Redis Cache	App Zone, AI Zone (DB port only)		Backup Zone only
<b>Integration Zone</b>	VAHAN/SARATHI Connector, FASTag Adapter, e-Challan Gateway	App Zone (internal API), NIC Gov Network		NIC Gov Network, e-Challan
<b>Security Zone</b>	SIEM, EDR Management Console, PAM, Vault	Management Zone only		All zones (monitoring read-only)
<b>Management Zone</b>	Bastion Host, Jump Server, CI/CD (build agents only)	Operator workstations (MFA + PAM)		All zones (admin ports)
<b>Backup Zone</b>	Backup Storage, DR Replication Targets	Data Zone (backup protocol only)		DR Site only
<b>LCCC Edge Zone</b>	LCCC Edge Servers, Local Cameras, VMS, Sensors	Field devices (ONVIF, MQTT, RTSP); RCC (WAN)		RCCC (encrypted WAN tunnel only)

**11.7. CERT-IN / MEITY COMPLIANCE****11.7.1. One-Time Compliance Activities**

Req ID	Requirement Description	Nature	Tier	Std / Ref
--------	-------------------------	--------	------	-----------

<b>FR-COMP-OT-001</b>	A comprehensive cybersecurity architecture review aligned with NCIIPC Critical Information Infrastructure protection guidelines shall be completed before system go-live, with the review report submitted to NHAI/IHMCL and NCIIPC as required.	<b>One-Time</b>	NCCC	NCIIPC CII
<b>FR-COMP-OT-002</b>	The platform shall be registered as a Critical Information Infrastructure (CII) system with NCIIPC before go-live, with all required documentation and technical information submitted per NCIIPC registration process.	<b>One-Time</b>	NCCC	NCIIPC CII Reg.
<b>FR-COMP-OT-003</b>	CERT-In mandatory compliance requirements shall be implemented before go-live: NTP-synchronised clocks on all systems (using government-approved NTP servers), 6-hour incident reporting capability, 180-day log retention operational, and point of contact registered with CERT-In.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-COMP-OT-004</b>	ISO 27001:2022 certification scope shall be defined and Stage 1 audit shall be completed within 6 months of go-live. Full certification (Stage 2 audit) shall be achieved within 18 months of go-live.	<b>One-Time</b>	NCCC	ISO 27001:2022
<b>FR-COMP-OT-005</b>	A pre-launch VAPT (Vulnerability Assessment and Penetration Testing) shall be conducted by a CERT-In empanelled organisation covering the entire platform (network, application, API, mobile, cloud infrastructure) before go-live. All Critical and High findings shall be remediated before SAC issuance.	<b>One-Time</b>	All	CERT-In Dir 2022
<b>FR-COMP-OT-006</b>	MeitY cloud empanelment compliance verification shall be completed for the selected CSP and specific cloud services before go-live. Evidence of MEITY empanelment of the CSP shall be included in the implementation completion documentation.	<b>One-Time</b>	NCCC	MEITY Cloud Policy
<b>FR-COMP-OT-007</b>	A Security Operations Centre (CSOC) with 24x7 operations shall be established before go-live, with documented SOPs for all security incident categories, escalation procedures, and CERT-In reporting workflows.	<b>One-Time</b>	NCCC	CERT-In Dir 2022

### 11.7.2. Annual Compliance Obligations

Req ID	Requirement Description	Nature	Tier	Std / Ref
--------	-------------------------	--------	------	-----------

<b>FR-COMP-ANN-001</b>	Annual VAPT shall be conducted by a CERT-In empanelled organisation covering the full platform scope. VAPT shall be completed within Q3 of each operational year. All Critical findings shall be remediated within 30 days and High findings within 90 days of the VAPT report.	Annual	All	CERT-In Dir 2022
<b>FR-COMP-ANN-002</b>	Annual ISO 27001 surveillance audit shall be conducted by the ISO 27001 certification body, maintaining continuous certification throughout the 10-year O&M period.	Annual	NCCC	ISO 27001:2022
<b>FR-COMP-ANN-003</b>	Annual third-party security audit of cloud infrastructure compliance against MeitY cloud security guidelines and CIS Cloud Benchmarks shall be conducted by a CERT-In empanelled organisation.	Annual	NCCC	MEITY Cloud Sec.
<b>FR-COMP-ANN-004</b>	Annual NCIIPC compliance review shall be conducted and a compliance report submitted to NCIIPC per their reporting schedule.	Annual	NCCC	NCIIPC CII
<b>FR-COMP-ANN-005</b>	Annual penetration testing of the RCCC, LCCC edge network (covering a representative sample of minimum 10% of LCCCs, rotated annually) shall be conducted to assess field network security posture.	Annual	LCCC	CERT-In Dir 2022
<b>FR-COMP-ANN-006</b>	Annual review and update of the Cybersecurity Incident Response Plan (CSIRP) shall be conducted, incorporating lessons learned from security incidents in the preceding year and changes in the threat landscape.	Annual	NCCC	ISO 27001 A.5.26
<b>FR-COMP-ANN-007</b>	Annual cybersecurity training and awareness programme shall be delivered to all ATMS platform operators, administrators, and management staff. Training completion records shall be maintained and provided to NHAI/IHMCL.	Annual	All	ISO 27001 A.6.3
<b>FR-COMP-ANN-008</b>	An annual Board-level cybersecurity risk report shall be prepared and presented to NHAI/IHMCL senior management, summarising the platform's security posture, significant incidents, residual risks, and planned improvements.	Annual	NCCC	ISO 27001 A.5.1

### 11.7.3. Cybersecurity License

License Category	License Scope
------------------	---------------

SIEM Platform License	Data ingestion capacity (EPS), log retention volume, user seats, threat intelligence feed subscriptions
EDR Platform License	Endpoint count (all NCCC, RCCC, LCCC servers + operator workstations). Includes threat intelligence feed and product updates.
NGFW / WAF License	Throughput license, IPS signature subscription, threat intelligence, SSL inspection capacity
VAPT Toolset License	Commercial scanning tools used by internal team (e.g., Nessus, Burp Suite Pro, Metasploit Pro)
Privileged Access Management (PAM)	Privileged user count, session recording storage
PKI / Certificate Management	SSL/TLS certificate management platform; number of managed certificates
Threat Intelligence Feed	Commercial threat intel subscriptions integrated with SIEM and NGFW
SAST / Code Analysis Tools	Static analysis tool licenses (per developer seat or per scan volume)
Vulnerability Management Platform	Asset count for continuous vulnerability scanning across all cloud and edge assets

## 12. TRAINING PROGRAMME OVERVIEW

An effective, comprehensive training programme is fundamental to the success of the National ATMS ICCC Platform. The platform's capabilities are only realised if the operators, supervisors, administrators, and partner agencies who use it are proficient, confident, and current in their skills. The Training Programme is not a one-time activity at go-live; it is a continuous, structured annual programme maintained throughout the 10-year O&M period.

The Training Programme is designed around five core principles: role-specific curricula (different content for different roles and tiers); blended learning (classroom, hands-on simulation, e-learning, and field exercises); continuous assessment (competency testing before and after training); annual refresh cycles (curriculum updated annually to reflect platform changes and emerging best practices); and training data transparency (all training records maintained in the platform and reported to NHAI/IHMCL).

### 12.1. Training Target Audience

User Group	Deployment Tier	Tentative Headcount	Training Priority
NCCC Operations Director / Deputy Director	NCCC	2–4	Executive / Leadership Training
NCCC Senior Operators	NCCC	10–15	Advanced Operator Training + Incident Command
NCCC Operators	NCCC	20–40	Core Operator Training
RCCC Directors / Senior Managers	RCCC (×20)	30–60	Leadership + Platform Overview
RCCC Senior Operators	RCCC (×20)	60–90	Advanced Operator Training
RCCC Operators	RCCC (×20)	180–300	Core Operator Training
LCCC Senior Operators	LCCC (×667+)	1,500–2,000	LCCC Operator + Device Management Training
LCCC Operators	LCCC (×667+)	3,000–6,000	Core LCCC Operator Training
System Administrators	NCCC / RCCC	10–20	Platform Administration Training
Enforcement Officers / Police Liaison	NCCC / RCCC / LCCC	200–500	Enforcement Workflow Training
Field Maintenance Technicians	LCC / Field	1,000–2,000	Field Device + Mobile App Training



Contractor / TSP Personnel	All	500–1,000	Contractor Portal + SLA Training
NHAI / IHMCL Management	NCCC	20–50	Executive Dashboard Training

## 12.2. INITIAL TRAINING PROGRAMME (IMPLEMENTATION PHASE)- (Online/Offline)

The initial training programme shall be delivered during Phase 3 and Phase 4 of the implementation timeline (Month 9 to Month 12), ensuring all operational staff are trained and competent before the system go-live date. Training shall be conducted in a dedicated training environment that mirrors the production platform configuration.

### 12.2.1. Training Modules – Initial Programme

Code	Training Module	Topics Covered	Duration	Target Audience
TRN-01	Platform Orientation and Common GUI Fundamentals	Platform overview; ICCC concept; hierarchy model; login & navigation; GIS map basics; dashboard layout; role-based views; multi-monitor setup; keyboard shortcuts; help system	1 day	All operators
TRN-02	GIS Map Operations	Map navigation; layer management; device interaction; incident icons; traffic flow layer; camera FOV overlay; drawing tools; geofence setup; map view presets; snapshot capture; search functions	1 day	All operators
TRN-03	Incident Detection and Management	Incident lifecycle; AI alert review; manual incident creation; SOP selection and execution; resource dispatch; VMS update from incident panel; escalation workflow; post-incident report; COP usage during incidents	2 days	NCCC/RCCC/LCCC operators
TRN-04	CCTV and Video Management	Live viewing; PTZ control; grid view; camera search; video playback; clip export; camera health indicators; NVR management; video wall control; evidence extraction	1 day	NCCC/RCCC/LCCC operators

<b>TRN-05</b>	VMS Management	Device overview; message library; manual message update; approval workflow; automated rule overview; cascade update; scheduling; audit log review	0.5 day	LCCC/RCCC operators
<b>TRN-06</b>	Enforcement Workflow	ANPR overview; violation detection; evidence review panel; challan approval; VAHAN query results; challan dispatch tracking; dispute workflow; watch-list management; enforcement dashboard	1 day	LCCC operators + enforcement
<b>TRN-07</b>	Traffic Monitoring and Analytics	Traffic flow layer; sensor data pop-ups; journey time display; congestion prediction layer; traffic analytics charts; report generation; incident-traffic correlation	0.5 day	NCCC/RCCC operators
<b>TRN-08</b>	Notifications, Alerts, and SOPs	Alert panel; severity levels; acknowledgement workflow; SOP builder introduction; SOP task completion; SOP compliance report	0.5 day	All operators
<b>TRN-09</b>	Collaboration Tools	Internal messaging; resource tasking; SMS/email notification dispatch; video conference from incident panel; shift handover procedure	0.5 day	All operators
<b>TRN-10</b>	Reporting and Dashboard Customisation	Standard report generation; ad-hoc report builder; dashboard widget configuration; scheduled report setup; export formats; KPI configuration	0.5 day	NCCC/RCCC supervisors
<b>TRN-11</b>	Advanced Operations (Senior Operators / Supervisors)	Major incident command; multi-agency coordination; emergency operations mode; escalation decision framework; SLA monitoring during incidents; post-incident debrief facilitation	1 day	Senior operators / supervisors
<b>TRN-12</b>	Platform Administration (System Admins)	User management; role configuration; device registry management; SOP builder; policy engine; GIS layer	2 days	System administrators

		management; integration monitoring; backup verification		
<b>TRN-13</b>	Cybersecurity Awareness	Password policy; MFA usage; phishing awareness; incident reporting obligation; data handling guidelines; CERT-In awareness; social engineering awareness	0.5 day	All users
<b>TRN-14</b>	Enforcement Officer / Police Liaison Training	Enforcement data access; challan evidence review; watch-list management; legal evidence export; VAHAN/SARATHI data interpretation; eCourts integration	1 day	Police liaison / enforcement
<b>TRN-15</b>	Field Technician Training	Mobile app usage; maintenance ticket management; QR code scanning; device status checking; fault logging; spare parts reporting	0.5 day	Field maintenance staff

#### 12.2.2. Training Delivery Methods

- Classroom / Instructor-Led Training (ILT): Preferred for core modules (TRN-01 to TRN-06). Delivered at training facility co-located with or adjacent to NCCC. Maximum batch size: 20 participants.
- Hands-On Simulation: All operator modules shall include minimum 40% hands-on time in the dedicated training environment. Operators shall complete simulated scenarios before assessment.
- E-Learning Modules: All modules shall have corresponding self-paced e-learning versions for remote access, hosted on the platform's integrated training module.
- Field Exercises: LCCC operator and field technician training shall include field exercises at a live LCCC site, covering on-site device inspection, camera PTZ operation, and incident simulation.
- Video-Recorded Demos: All training modules shall have narrated screen-recording demos accessible through the platform's training module for self-revision.

#### 12.2.3. Training Assessment and Certification

All training modules shall include a competency assessment: a pre-training knowledge check (baseline), and a post-training assessment (minimum 60% pass mark required). Participants who fail the post-training assessment shall receive remedial coaching and a re-test within 5 working days. Operators shall not be permitted to commence live operational duties without passing the relevant module assessments.

A Training Completion Certificate shall be issued to each participant upon successful completion of all required modules for their role. Certificates shall be recorded in the platform's training management sub-module, accessible to NHAI/IHMCL supervisors. A Master Training Register shall be maintained by the System Integrator and submitted to NHAI/IHMCL quarterly.

### 12.3. ANNUAL TRAINING PROGRAMME (O&M PHASE)

The Annual Training Programme shall be delivered each operational year throughout the 10-year O&M period. The programme covers: refresher training for existing operators; induction training for new joiners; specialised training for platform enhancements; leadership training for senior management; and tabletop exercises for emergency scenario preparedness.

#### 12.3.1. Annual Training Calendar

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-TRN-ANN-001</b>	Annual Operator Refresher Training shall be delivered to all NCCC, RCCC, and LCCC operators (all tiers) in Q1 of each operational year. Refresher training shall cover: platform updates from the preceding year, lessons learned from major incidents, SOP updates, and regulatory updates. Minimum 1 day per operator per year.	Annual	All	Training Programme
<b>FR-TRN-ANN-002</b>	New Joiner Induction Training shall be delivered to all new operators, administrators, and maintenance staff within 30 days of joining. New joiners shall not be assigned unsupervised operational duties until induction training and assessment is completed.	Annual	All	HR + Training
<b>FR-TRN-ANN-003</b>	Platform Enhancement Training shall be delivered for every major platform release, covering all new or changed features, workflows, and integrations. Delivery shall be timed to align with or precede the platform upgrade.	Annual	All	DEST Team
<b>FR-TRN-ANN-004</b>	Advanced Incident Management Tabletop Exercise shall be conducted bi-annually at NCC level, simulating major incident scenarios (multi-vehicle accident, wrong-way driving, highway flooding, ransomware attack). Exercise shall include NCCC, at least 3 RCCs, and 5 LCCCs in a coordinated simulation.	Annual	NCCC/RCCC/LCCC	Emergency Preparedness
<b>FR-TRN-ANN-005</b>	Cybersecurity Awareness Training (annual refresh) shall be delivered to all platform users, covering updated phishing techniques, social engineering, CERT-In obligations, and the year's	Annual	All	ISO 27001 A.6.3

	notable security incidents (anonymised). Minimum 2 hours; assessed via quiz.			
<b>FR-TRN-ANN-006</b>	Enforcement Officer Training Update shall be delivered annually to all enforcement officers and police liaison personnel, covering: legal updates (amendments to MV Act), new violation types detected by the platform, evidence handling procedures, and court testimony guidance.	Annual	NCCC/RCCC/LCCC	Legal compliance
<b>FR-TRN-ANN-007</b>	Field Technician Certification Renewal shall be conducted annually for all field maintenance technicians, covering new device types commissioned in the preceding year, updated maintenance procedures, and health and safety refresher.	Annual	LCCC/Field	ATMS field ops
<b>FR-TRN-ANN-008</b>	NHAI/IHMCL Management Awareness Session shall be conducted annually, providing senior management with an overview of: platform performance against KPIs, significant incidents and lessons learned, technology developments (AI, cloud, cybersecurity), and the O&M roadmap for the coming year. Duration: 0.5 day.	Annual	NCCC	Stakeholder engagement
<b>FR-TRN-ANN-009</b>	Train-the-Trainer Programme shall be conducted annually, certifying minimum 5 NHAI/IHMCL personnel as platform trainers capable of delivering Tier 1 operator training modules independently. Certified trainers shall be re-certified every 3 years.	Annual	NCCC	Capacity building
<b>FR-TRN-ANN-010</b>	Disaster Recovery and Business Continuity Exercise shall be conducted annually at LCC level (representative sample: 10% of LCCs, rotated), simulating LCC edge autonomy scenarios (WAN outage, server failure, power failure) and validating operator proficiency in autonomous LCC operations.	Annual	LCCC	BC/DR preparedness

### 12.3.2. Annual Training Requirements – By Role

Role	Annual Refresher	Enhancement Training	Cybersecurity	Total Minimum Days/Year
NCCC Operations Director	0.5 day (executive)	Per release (0.5 day)	2 hours (e-learn)	1 day
NCCC / RCCC Senior Operator	1 day (refresher + tabletop)	Per major release (1 day)	0.5 day	2.5 days
NCCC / RCCC Operator	1 day (refresher)	Per major release (0.5 day)	0.5 day	2 days
LCCC Senior Operator	1 day (refresher)	Per major release (0.5 day)	0.5 day	2 days
LCCC Operator	1 day (refresher)	Per major release (0.5 day)	0.5 day	2 days
System Administrator	1 day (advanced)	Per release (1 day – technical)	1 day (deep-dive)	3 days
Enforcement Officer	1 day (incl. legal update)	Per major release (0.5 day)	2 hours (e-learn)	2 days
Field Maintenance Technician	1 day (incl. new devices)	Per major release (0.5 day)	2 hours (e-learn)	2 days
TSP Contractor Personnel	0.5 day (SLA/portal update)	Per major release (0.5 day)	2 hours (e-learn)	1 day

### 12.3.3. Training Infrastructure Requirements

Req ID	Requirement Description	Nature	Tier	Std / Ref
<b>FR-TRN-INFRA-001</b>	The platform shall include an integrated Training Management Sub-Module within the Common GUI enabling administrators to: schedule training sessions, enrol participants, track attendance, record assessment results, issue digital training certificates, and generate training compliance reports.	<b>One-Time</b>	NCCC	Platform training module

<b>FR-TRN-INFRA-002</b>	A dedicated training environment (separate from production, UAT, and development) shall be maintained throughout the 10-year O&M period, with the same platform version as production deployed within 5 business days of any production upgrade.	<b>OT/CONT</b>	NCCC	Training infra
<b>FR-TRN-INFRA-003</b>	A minimum library of 50 realistic operational scenarios shall be available in the training environment, covering all major incident types, enforcement workflows, and emergency scenarios. The scenario library shall be updated annually.	<b>OT/ANN</b>	NCCC	Scenario library
<b>FR-TRN-INFRA-004</b>	All training modules shall have corresponding e-learning versions hosted on the platform's training module, accessible by all registered users from any device with platform access.	<b>One-Time</b>	NCCC	E-learning
<b>FR-TRN-INFRA-005</b>	Training completion rates and assessment pass rates shall be reported to NHAI/IHMCL quarterly. Any role category with a training completion rate below 80% shall trigger a mandatory remedial plan submitted within 30 days.	<b>Annual</b>	NCCC	Training governance
<b>FR-TRN-INFRA-006</b>	A Master Training Calendar for each operational year shall be submitted to NHAI/IHMCL for approval by Month 11 of the preceding year, detailing all planned training activities, schedules, venues, and expected participant counts.	<b>Annual</b>	NCCC	Training governance
<b>FR-TRN-INFRA-007</b>	Video-recorded versions of all training module deliveries shall be made available within 10 business days of delivery through the platform's training module, enabling absent participants to self-study and be assessed remotely.	<b>OT/CONT</b>	NCCC	Training access
<b>FR-TRN-INFRA-008</b>	The System Integrator shall provide a minimum of 5 training days per year of on-site training support at NCCC, and at least 2 training days per year of on-site support at each RCCC (or as agreed per zone with NHAI/IHMCL).	<b>Annual</b>	NCCC/RCCC	Training delivery



**12.4. TRAINING – FUNCTIONAL REQUIREMENTS SUMMARY**

Req ID	Requirement	Priority
<b>FR-TRN-001</b>	The platform shall include an integrated training management sub-module supporting scheduling, enrolment, attendance tracking, assessment recording, certificate issuance, and compliance reporting for all training programmes.	<b>P1</b>
<b>FR-TRN-002</b>	All platform operators shall complete the role-appropriate initial training programme and pass all competency assessments before being permitted to undertake unsupervised live operational duties.	<b>P1</b>
<b>FR-TRN-003</b>	The training environment shall be maintained throughout the 10-year O&M period with the current production platform version, updated within 5 business days of any production upgrade.	<b>P1</b>
<b>FR-TRN-004</b>	The training module shall support SOP simulation mode, enabling operators to practice SOP execution in simulated incident scenarios without creating real incidents or triggering real notifications.	<b>P1</b>
<b>FR-TRN-005</b>	A minimum of 50 realistic scenario scripts shall be developed for the training environment at go-live, updated with minimum 10 new scenarios annually during O&M.	<b>P1</b>
<b>FR-TRN-006</b>	Annual refresher training shall be delivered to all operators within Q1 of each operational year, with training completion reports submitted to NHAI/IHMCL by the end of Q1.	<b>P1</b>
<b>FR-TRN-007</b>	The System Integrator shall conduct bi-annual major incident tabletop exercises involving NCC, minimum 3 RCCCs, and 5 LCCCs simultaneously, with exercise reports and lessons learned submitted to NHAI/IHMCL.	<b>P1</b>
<b>FR-TRN-008</b>	A Train-the-Trainer programme shall be conducted annually, certifying minimum 5 NHAI/IHMCL personnel as platform trainers to build internal training capability and reduce long-term dependency on the System Integrator.	<b>P2</b>
<b>FR-TRN-009</b>	The training management sub-module shall generate a quarterly training compliance dashboard showing: percentage of operators trained by role and tier, assessment pass rates, upcoming training deadlines, and overdue training.	<b>P1</b>
<b>FR-TRN-010</b>	All training materials (user guides, quick reference cards, e-learning modules, scenario scripts) shall be updated within 30 days of any major platform release and made available through the platform's training module.	<b>P1</b>

<b>FR-TRN-010</b>	<p>The ATMS platform shall provide a <b>dedicated “Training Calendar” module/tab</b> for each tier, displaying a consolidated schedule of <b>completed, ongoing, and upcoming trainings</b>.</p> <p>The module shall include:</p> <ul style="list-style-type: none"><li>• Training details such as <b>date, time, location, and target participants</b></li><li>• Status tracking (completed/upcoming)</li><li>• Access to <b>training materials (soft copies)</b> through embedded links or downloadable repository</li></ul> <p>The system shall ensure <b>easy navigation, role-based access, and centralized availability</b> of all training-related information for effective capacity building and knowledge management.</p>	<b>P1</b>
-------------------	---	-----------

### 13. BILL OF QUANTITIES (BoQ) FRAMEWORK

All quantities are indicative for pricing reference; actual quantities shall be governed by the programme deployment schedule and approved by IHMCL. **IMPORTANT: This BoQ does not contain financial values. No financial figures should appear in the Technical Bid.**

#### 13.1. WP-1 — Core Platform Architecture & Development (Years 1–5)

BoQ Item	Description	Unit	Qty (Indicative)
WP1-01	Core ATMS Event and Incident Processing Engine — Design, development, testing, and stabilization	Lump Sum	1
WP1-02	Unified National GIS-Based ATMS Control Platform — National, regional, and corridor dashboards	Lump Sum	1
WP1-03	All external government/agency integrations operational and acceptance-tested: VAHAN, SARATHI, FASTag/NETC, CCTNS, iCAD, Rajmarg, NHAI App, NERS 112, eCourts, IMD, DMC/SDMA, State ICCCs, Police PCR, AIS-140, DigiLocker, PM Gati Shakti, IHMCL DataLake, NIC Enforcement Portal. Additional integrations may be required as per project requirements during project tenure.	Lump Sum	1
WP1-04	All Existing Field Platform Vendor API interfaces (VIDES, ANPR/TTMS, VMS, Radar, VASD, enforcement/e-Challan, Vendor NMS, ATCC) operational per DES (Data Exchange Specification)	Lump Sum	1
WP1-05	Traffic Data Lake, Streaming, and Analytics Platform — Data lake architecture, ETL pipelines, analytics platform	Lump Sum	1
WP1-06	IAM, MFA, ZTA, SIEM (CERT-In compliant), EDR, IDS/IPS, DLP, PAM, NAC, network micro-segmentation, encryption, audit logging — all operational at NCCC/RCCC/LCCC	Lump Sum	1
WP1-07	Full Integrated Audio Communication Engine — ECB/1033 integration, call recording, in-platform messaging, PTT/radio integration	Lump Sum	1
WP1-08	iOS and Android field operator app	Lump Sum	1

WP1-09	Progressive web app with externally published APIs for third party sites to showcase road information	Lump Sum	1
WP1-10	Data Fusion and alerts engine	Lump Sum	1
WP1-11	Full-scale performance validated (100K+ devices, 10M+ vehicles/day); DR test passed (RTO<2hr, RPO<4hr); initial VAPT cleared	Lump Sum	1
WP1-12	CI/CD pipelines, IaC codebase, observability stack, and OEM sandbox environment operational and Software Operation & Maintenance	Lump Sum (Yrs 2 - 5)	4
WP1-13	PMO, change management process, release cadence, SRS baseline, RTM, SBOM, and all required project documentation	Lump Sum (Yrs 2 - 5)	4

### 13.2. WP-2 — Software Enhancements & Product Evolution (Years 6–10)

BoQ Item	Description	Unit	Qty (Indicative)
WP2-01	Enhancement Retainer — Years 6–8:	Per Year	3
WP2-02	Enhancement Retainer — Years 9–10: Reduced team	Per Year	2

### 13.3. WP-3 — Deployment & Corridor Integrations (Years 1–10)

BoQ Item	Description	Unit	Qty (Indicative)
WP3-01	Deployment and Readiness at each Locations of LCCC, RCCC and NCCC (including Cloud + On-Prem DC integrated) Indicative Locations: LCCC = 667, RCCC = 20 and NCCC = 1	Per Unit (location)	688

### 13.4. WP-4 — Operations & Maintenance (Years 1–10)

BoQ Item	Description	Unit	Qty (Indicative)
WP4-01	O&M Service — Years 2–3: Full O&M team	Per Year	2
WP4-02	O&M Service — Years 4–7: O&M team (adjusted Year 4–7 profile)	Per Year	4

WP4-03	O&M Service — Years 8–10: O&M team (reduced profile)	Per Year	3
WP4-04	Annual DR Test — Full failover simulation, RTO/RPO validation (RTO <4 hrs, RPO <2 hr)	Per Year	9

### 13.5. WP-5 — Training, Compliance & Specialized Tools

BoQ Item	Description	Unit	Qty (Indicative)
WP5-01	ATMS Platform Training Programmes (Online/Offline) — Design, development, and delivery.	Per Programme	20
WP5-02	Cybersecurity VAPT by CERT-In Empanelled Auditor — Per assessment (minimum 10 over contract).	Per Assessment	10
WP5-03	Compliance Certification — ISO 27001, STQC, MeitY, NCIIPC assessments.	Per Assessment	5
WP5-04	Specialized Engineering and Security Tools — SAST/DAST/API Security/Observability tool licensing and maintenance.	Per Year	9

---

**SCHEDULE A — SERVICE LEVEL AGREEMENT**

---

**1. Key Terms and Definitions**

---

**1.1. Platform Availability / Uptime**

Platform Availability refers to the proportion of calendar time during which the ATMS Platform — comprising the National Command Control Centre (NCCC), all commissioned Regional Command Control Centres (RCCCs), and all commissioned Local Command Control Centres (LCCCs) — are fully operational, accessible, and able to process traffic data without degradation. It is expressed as a percentage of the total time in a calendar month, excluding pre-approved scheduled maintenance windows notified at least 72 hours in advance.

**Formula: Availability (%) = (Total Minutes in Month – Unplanned Downtime Minutes) / Total Minutes in Month) × 100**

**1.2. National Command & Control Centre (NCCC)**

The NCCC is the apex control facility responsible for system-wide monitoring, data aggregation, strategic traffic management, and coordination with national authorities including IHMCL, NHAI, and law enforcement. NCCC availability is held to a higher standard (99.9% monthly) because its failure disrupts all downstream RCCC and LCCC operations.

**1.3 Regional Command & Control Centre (RCCC)**

Each RCCC is a sub-national control facility managing a defined geographic zone of the ATMS network. The RCCC aggregates data from its associated LCCCs, manages field device coordination, and relays enforcement data to government integration endpoints. A single RCCC failure triggers a P2 fault.

**1.4 Local Command & Control Centre (LCCC)**

LCCCs are edge nodes that directly interface with field equipment: cameras, variable message signs (VMS), loop detectors, ANPR readers, and roadside units (RSUs). The LCCC Online Rate is the percentage of all commissioned LCCCs that are online and responsive at any point in time. More than 5% offline triggers P2; more than 20% offline triggers P1.

**1.5 Incident Response Time**

Incident Response Time is the elapsed duration from the moment a fault is logged (automatically or manually) in the Incident Management System (IMS) to the moment a qualified engineer acknowledges the incident, begins active investigation, and records the first remediation action in the IMS. This is distinct from resolution — response is the act of engaging the problem, not solving it.

---

### 1.6 Incident Resolution Time

Incident Resolution Time is the elapsed duration from the fault log timestamp to the moment the system or sub-system is restored to full, verified operational status and the incident is formally closed in the IMS with post-remediation validation. Resolution requires documented root-cause analysis (RCA) for all P1 and P2 incidents.

### 1.7 Data Processing Latency

Data Processing Latency is the end-to-end elapsed time from the moment a field sensor (loop detector, ANPR reader, CCTV, RSU) captures an event to the moment that event is reflected on the NCCC dashboard in a viewable and actionable form. The P95 (95th percentile) latency must remain below 3 seconds in any calendar month, meaning 95% of all data transactions must complete within this window.

### 1.8 Disaster Recovery — RTO and RPO

Recovery Time Objective (RTO) is the maximum acceptable elapsed time between a declared full system failure (primary Data Centre outage) and the complete restoration of ATMS services from the Disaster Recovery (DR) site. The RTO is 2 hours.

Recovery Point Objective (RPO) is the maximum acceptable amount of data loss, measured in time, that can result from a full system failure. An RPO of 4 hours means that in the worst case, no more than 4 hours of transactional data (sensor readings, enforcement records, incident logs) may be irrecoverably lost. This is achieved through continuous or near-continuous data replication to the DR site.

### 1.9 SIEM and CSOC

The Security Information and Event Management (SIEM) system continuously monitors all ATMS network, application, and operating system logs for security anomalies, intrusion attempts, and policy violations. The Cyber Security Operations Centre (CSOC) is the team staffed 24×7 responsible for monitoring SIEM alerts and executing the incident response process. The Mean Time to Respond (MTTR) for P1 SIEM alerts is capped at 15 minutes.

### 1.10 CERT-In Reporting Obligation

Under Section 70B of the Information Technology Act, 2000, and the CERT-In Directions (April 2022), any reportable cyber security incident affecting critical information infrastructure — including national highway traffic management systems — must be reported to the Indian Computer Emergency Response Team (CERT-In) **within 6 hours** of detection. Failure to report within this window constitutes a P1 contract breach with potential regulatory consequences including fines and suspension.

### 1.11 Government Integration Uptime

The ATMS is integrated with the following government databases and enforcement platforms but not only limited to:

- VAHAN — MoRTH vehicle registration database
- SARATHI — driving licence database
- FASTag / NETC — electronic toll collection and vehicle tracking



- 
- e-Challan — centralised traffic violation management system
  - State Police — FIR linking and enforcement coordination
  - eCourts — adjudication pipeline for contested challans
  - State ICCCs — Integration with State Integrated Command and Control Centres
  - Rajmatra App
  - CCTNS

Each integration must maintain 99% monthly uptime. Failure of any single integration triggers a P2 fault and is escalated to IHMCL.

### 1.12 Security Patch Deployment

A Critical CVE (Common Vulnerabilities and Exposures) is any publicly disclosed software vulnerability assigned to a CVSS (Common Vulnerability Scoring System) Base Score of 9.0 or above. Such vulnerabilities represent the highest risk of system compromise, data breach, or service disruption. The Contractor is obligated to deploy patches for all Critical CVEs across all ATMS components within 72 hours of the vulnerability's public disclosure on the National Vulnerability Database (NVD) or vendor advisory. 100% compliance is mandatory; no exceptions are permitted without written Director-level waiver.

### 1.13 Annual DR Test

Once per year, during Q4 of each O&M year, the Contractor shall conduct a full, live Disaster Recovery Simulation. This test involves a controlled shutdown of the on premises NCCC primary Data Centre and a complete failover to the cloud DR site, with all ATMS services being restored within the RTO (<2 hours) and data integrity verified to be within the RPO (<4 hour of loss). The test result must be 'Pass'. A 'Fail' result requires submission of a formal Remediation Plan within 30 days and triggers a P1 escalation to Director level.

### 1.14 Annual Operator Training Compliance

All active ATMS operators — including NCCC, RCCC, and LCCC control room staff — must complete their annual refresher training programme by the end of Q1 (i.e., 31 March) of each O&M year. The training curriculum covers system updates, emergency protocols, enforcement procedures, cybersecurity awareness, and equipment handling. Non-compliance triggers a Training Compliance Report Escalation and is treated as a contractual default under the O&M Agreement.

## 2. SLA GOVERNANCE FRAMEWORK

### 2.1 Measurement Architecture

All SLA parameters are measured continuously via the ATMS Operations Dashboard. Automated health probes query each NCCC, RCCC, and LCCC instance at 5-minute intervals. IHMCL has read-only access to the dashboard at all times. The IA (Implementation Agency) maintains the SLA monitoring engine as part of WP-4 O&M obligations.

### 2.2 Monthly SLA Report

**Due:** Within 5 business days of each calendar month-end. The Monthly SLA Report must include:

- Actual vs. target performance for all 17 SLA parameters with numerical evidence.
- Incident log (all P1–P3 incidents): creation timestamp, acknowledgement timestamp, resolution timestamp, duration.
- RCA submissions: full RCA for all P1 closures (due within 48 hours of closure); RCA summary for P2 closures (due within 72 hours).
- Penalty computation: self-calculated SLA deductions per parameter, itemised by incident.
- Vulnerability and patch status: all open CVEs by severity, patch deployment dates.
- DR replication lag monitoring: average and maximum replication lag for the month.
- Integration uptime: per-integration availability percentage for all 10+ external integrations.

### 2.3 SLA Deduction Mechanics — Monthly to Quarterly

Step	Process
Step 1 — Monthly Measurement	SLA performance measured continuously; monthly metrics compiled in the Monthly SLA Report.
Step 2 — Monthly Penalty Calculation	IA self-calculates penalties per parameter per month. IHMCL verifies or disputes within 10 business days.
Step 3 — Quarterly Accumulation	Monthly penalties for Months 1, 2, 3 of a quarter are summed.
Step 4 — Pro-Rata Adjustment	Penalties are applied against the pro-rata quarterly OPEX (not the full rate).
Step 5 — Payment Gate Check	Before releasing payment: (a) uptime $\geq 99.5\%$ for each month in quarter; (b) no P1/P2 breach open $>7$ days; (c) valid DSC issued.

Step	Process
Step 6 — Invoice Settlement	IHMCL deducts accumulated penalties from the quarterly invoice. Net payment released within 30 days.
Step 7 — Monthly Cap Check	Total deductions in any single calendar month may not exceed 20% of that month's pro-rata OPEX. This cap is applied before quarterly accumulation.

### 3. COMPLETE SLA PARAMETER REGISTER

All 17 binding SLA parameters across 7 categories. Each parameter is aligned to the applicable WP, the payment impact, and the measurement source.

**Table 3.1 — SLA Parameter Quick Reference**

SLA ID	Category	Parameter	WP Scope	Target	Penalty Basis	Payment Impact
SLA-01	A	Platform Availability	WP-4 O&M	≥99.5%/month	Tiered % of monthly OPEX	Payment hold if <99.0%
SLA-02	A	NCCC Availability	WP-4 O&M	≥99.9%/month	0.5% OPEX/hr downtime	P1 escalation ≥1 hr downtime
SLA-03	A	RCCC Availability (each)	WP-4 O&M	≥99.5%/month	0.25% OPEX/4-hr breach	Max 10% OPEX across all RCCCs
SLA-04	A	LCCC Online Rate	WP-3 + WP-4	≥98% at all times	INR 10K/LCCC/day	Capped at 10% monthly OPEX
SLA-05	B	P1 Incident Response	WP-4 O&M	≤15 min	0.5% OPEX/hr delay	Capped at 10% monthly OPEX
SLA-06	B	P1 Incident Resolution	WP-4 O&M	≤4 hrs	0.5% OPEX/hr delay	Capped at 10% monthly OPEX
SLA-07	B	P2 Incident Response	WP-4 O&M	≤30 min	0.25% OPEX/4-hr block	Capped at 10% monthly OPEX
SLA-08	B	P2 Incident Resolution	WP-4 O&M	≤8 hrs	INR 5K/4-hr block	Capped at 10% monthly OPEX
SLA-09	C	Data Processing Latency	WP-1 + WP-4	P95 <3s	INR 10K/hr breach	Capped 50K/month INR
SLA-10	D	SIEM P1 MTTR	WP-4 + WP-1(06)	<15 min MTTR	0.5% OPEX/hr cumulative	Capped at 10% monthly OPEX

SLA ID	Category	Parameter	WP Scope	Target	Penalty Basis	Payment Impact
SLA-11	D	CERT-In Reporting	WP-4 + WP-5(02)	≤6 hrs from detection	INR 5,00,000 per late filing	Full IA liability for MeitY penalties
SLA-12	E	Govt Integration Uptime	WP-1(03) + WP-4	≥99%/integration/month	INR 5K/hr/integration	Capped INR 50K/integration/month
SLA-13	F	DR RTO	WP-4(04) DR Test	<2 hrs	0.5% OPEX/hr beyond RTO	10% monthly OPEX cap/event
SLA-14	F	DR RPO	WP-4(04) DR Test	<4 hrs	0.5% OPEX/30 min excess	Performance Security trigger
SLA-15	F	Annual DR Test Result	WP-4(04)	PASS (both RTO+RPO)	INR 5,00,000 + re-test at IA cost	2 consec. failures = Event of Default
SLA-16	G	Security Patch Deployment	WP-4 + WP-5	100% Critical CVE ≤72 hrs	INR 1L/day Critical; INR 25K/day High	Critical >7 days = Event of Default
SLA-17	G	Operator Training Compliance	WP-5(01)	100% by 31 March/yr	INR 10K/operator/week delay	Default if <90% by 30 April

### 3.1 Category A — Platform Availability

#### SLA-01 | Platform Availability [Category A | WP-4 O&M]

<b>Definition</b>	Overall uptime of the National ATMS Software Platform — NCCC + all active RCCCs + all commissioned LCCCs. An instance is "up" when accessible to operators, processing live field data, and transmitting events through the command hierarchy.
<b>Target</b>	≥ 99.5% in any calendar month. Availability % = (Total uptime minutes of all instances ÷ Total possible minutes) × 100
<b>Measurement</b>	Automated health probes at 5-minute intervals per instance. Real-time dashboard accessible to IHMCL. Reported monthly within 5 business days of month-end.

<b>Exclusions</b>	<p>(1) Planned maintenance ≤4 hrs/instance/month with 72-hr notice;</p> <p>(2) Force Majeure;</p> <p>(3) Outages solely from on-premise hardware failure (SI responsibility);</p> <p>(4) Government-directed network shutdown.</p>
<b>Penalty Tiers</b>	<p><b>Tier 1 (99.0%–99.5%):</b> 2% of monthly OPEX per 0.1% shortfall below 99.5% — capped at 10% of monthly OPEX.</p> <p><b>Tier 2 (98.0%–99.0%):</b> 5% of monthly OPEX per 0.1% shortfall below 99.0% — capped at 15% of monthly OPEX.</p> <p><b>Tier 3 (&lt;98.0%):</b> 15% of monthly OPEX flat deduction. Critical Breach — IHMCL Board notification mandatory. 3 consecutive Critical Breaches = Event of Default (Volume 3, Section 7).</p>
<b>WP Link</b>	<p><b>Payment</b> Uptime ≥99.5% is a MANDATORY condition for WP-4 quarterly payment release (payment terms 4.1/4.2/4.3).</p> <p>A Critical Breach (Tier 3) triggers a payment hold until remediated and IHMCL issues a clearance note.</p>

**SLA-02 | NCCC Availability** [Category A | WP-4 O&M]

<b>Definition</b>	Availability of the NCCC platform (on-premise DC + Cloud DR). Available when: NCCC dashboard accessible, data ingestion active from all RCCCs, national GIS layer live, and API gateway responding.
<b>Target</b>	≥ 99.9% in any calendar month.
<b>Measurement</b>	5-minute automated probes on NCCC dashboard URL, API gateway health endpoint, and IT infrastructure health check. Live infrastructure dashboard for IHMCL.
<b>Exclusions</b>	<p>(1) Planned maintenance ≤2 hrs/month with 72-hr notice;</p> <p>(2) CSP-wide infrastructure outages (CSP status page confirmed);</p> <p>(3) Force Majeure;</p> <p>(4) NCCC operator workstation failures (IHMCL-procured).</p>
<b>Penalty</b>	<p>0.5% of monthly OPEX per hour of NCCC downtime beyond the 99.9% threshold. Director-level escalation mandatory if NCCC downtime exceeds 1 continuous hour. NCCC availability &lt;99.5% in any month also triggers SLA-01 Tier 1 deduction.</p>

**SLA-03 | RCCC Availability (Per RCCC)** [Category A | WP-4 O&M]

<b>Definition</b>	Availability of each individual RCCC instance (compute, storage, application stack, dashboard). 20 RCCCs total. Each measured independently.
<b>Target</b>	≥ 99.5% per individual RCCC per calendar month.
<b>Measurement</b>	5-minute probes per RCCC. Zonal dashboard with per-RCCC uptime. Failure of one RCCC does not affect another's SLA.
<b>Exclusions</b>	(1) Planned maintenance ≤2 hrs/RCCC/month with 72-hr notice; (2) IT infrastructure outages confirmed by Zonal Team; (3) Force Majeure; (4) IHMCL-directed zone reconfiguration.
<b>Penalty</b>	0.25% of monthly OPEX per 4-hour breach per affected RCCC. P2 fault per non-compliant RCCC. If >3 RCCCs breach in same month: P1 escalation and Director-level review. Cumulative cap: 10% of monthly OPEX across all RCCCs.

**SLA-04 | LCCC Online Rate** [Category A | WP-3 Deployment + WP-4 O&M]

<b>Definition</b>	% of commissioned LCCCs online and operational (communicating with field devices and transmitting data to the RCCC) at any given time.
<b>Target</b>	≥ 98% of commissioned LCCCs online at all times. Reported as monthly average and minimum recorded in any 1-hour window during the month.
<b>Measurement</b>	LCCC agent heartbeat every 5 minutes. LCCC classified "offline" if no heartbeat for >15 continuous minutes. Automated alert if rate drops below 99% (warning) or 98% (breach).
<b>Exclusions</b>	(1) Planned maintenance at individual LCCC with 24-hr notice; (2) LCCC hardware failure (SI responsibility); (3) LCCC connectivity outage (IHMCL/SI procured); (4) Force Majeure.
<b>Penalty</b>	<98% to ≥95% online: P2 fault; INR 5,000 per LCCC offline per day beyond SLA. Capped at 5% monthly OPEX.



	<p><b>&lt;95% online:</b> P1 fault; INR 10,000 per LCCC offline per day; Director-level escalation; remediation plan required within 24 hours.</p> <p>Capped at 10% monthly OPEX.</p> <p><i>Note: LCCC online rate is linked to WP-3 deployment pace. Only commissioned LCCCs (per DSC) count in the denominator.</i></p>
--	---

### 3.2 Category B — Incident Response & Resolution

#### SLA-05 | P1 Incident Response Time [Category B | WP-4 O&M]

<b>Definition</b>	Elapsed time from P1 IMS ticket creation to first active SDA NOC acknowledgement (ticket acknowledged, named engineer assigned, initial assessment posted in IMS).
<b>Target</b>	≤ 15 minutes from IMS ticket creation timestamp.
<b>P1 Triggers</b>	NCCC platform fully down; >20% commissioned LCCCs offline simultaneously; major cyber incident; enforcement pipeline completely down; DC failure with DR not activated within RTO; data lake ingestion failed >30 min; SIEM P1 confirmed malicious activity.
<b>Measurement</b>	IMS auto-timestamps ticket creation and first NOC action. Auto-escalation to IA NOC Manager + IHMCL Duty Officer if no acknowledgement within 10 minutes.
<b>Penalty</b>	<p>0.5% of monthly OPEX per hour (or part thereof) of delay beyond 15-minute SLA.</p> <p>If response exceeds 30 minutes: auto-escalation to IA Director and IHMCL Technical Director.</p> <p>Capped at 10% of monthly OPEX.</p>

#### SLA-06 | P1 Incident Resolution Time [Category B | WP-4 O&M]

<b>Definition</b>	Elapsed time from P1 IMS ticket creation to full platform restoration (automated health checks passed + IHMCL operator sign-off + preliminary RCA posted in ticket).
<b>Target</b>	≤ 4 hours from IMS ticket creation. Full RCA document within 48 hours of resolution.
<b>War-Room Rule</b>	If P1 not resolved within 2 hours: mandatory war-room call — IA Incident Commander, IA Senior Engineers, IHMCL Technical Director, Cloud Architect, IHMCL CISO (if cyber). Status updates every 30 minutes.

<b>Penalty</b>	0.5% of monthly OPEX per hour beyond 4-hour SLA. Example: resolution at 7 hrs = 3 hrs × 0.5% = 1.5% deduction. Capped at 8% of monthly OPEX across all P1 resolution failures in the month.
<b>Escalation (Full)</b>	T+0: IA NOC Manager + IHMCL Duty Officer (auto). T+15 min: IA Director if not acknowledged. T+30 min: War-room. T+2 hrs: IHMCL CEO/Executive Director. Cyber: CERT-In within 6 hours.
<b>Repeated Breach</b>	≥3 P1 resolution breaches in any 3 consecutive months: formal Performance Review; potential Performance Security invocation (Clause 5.3).

**SLA-07 | P2 Incident Response Time** [Category B | WP-4 O&M]

<b>Target</b>	≤ 30 minutes from IMS ticket creation timestamp.
<b>P2 Triggers</b>	Single RCCC fully down; >5% but ≤20% LCCCs offline; enforcement pipeline degraded; GIS map unavailable at NCCC/RCCC; AI inference engine fully down; DR replication lag 15–60 min; >3 Government integration endpoints down; data latency >10s for >1 hour; SIEM P1 alert unconfirmed.
<b>Penalty</b>	0.25% of monthly OPEX per 4-hour block of delay beyond 30-minute SLA. Capped at 10% of monthly OPEX. Escalation to IHMCL Senior Manager if P2 response exceeds 1 hour.

**SLA-08 | P2 Incident Resolution Time** [Category B | WP-4 O&M]

<b>Target</b>	≤ 8 hours from IMS ticket creation. Full RCA within 72 hours of resolution.
<b>Penalty</b>	INR 5,000 per 4-hour block of delay beyond 8-hour SLA. Example: resolution at 18 hrs = 10 hrs beyond SLA = 2.5 blocks × INR 5,000 = INR 12,500 per incident. Capped at 10% of monthly OPEX.
<b>Escalation</b>	T+6 hrs (2 hrs before SLA): IHMCL notified of estimated resolution time. Written holding note with revised ETA required if SLA breach anticipated. P2 may be escalated to P1 if: (a) >20% LCCCs affected; (b) confirmed security breach; (c) persists beyond 8 hours.

<b>Repeated Breach</b>	≥5 P2 resolution breaches in any single month: mandatory O&M Manager + IHMCL Senior Manager performance review.
------------------------	---

### 3.3 Category C — Software Performance

#### SLA-09 | Data Processing Latency [Category C | WP-1(01-05) + WP-4 O&M]

<b>Definition</b>	95% end-to-end latency: from field sensor event at LCCC edge to appearance on NCCC dashboard, covering the full pipeline (LCCC edge → RCCC → NCCC dashboard rendering).
<b>Target</b>	Latency < 3 seconds, measured continuously on a rolling 1-hour window.
<b>Measurement</b>	Platform-embedded pipeline monitoring. Every event timestamped at LCCC edge and NCCC receipt. Alert if > 2.5s (warning) or > 3s for >15 consecutive minutes.
<b>Penalty</b>	<p><b>3–5 seconds:</b> INR 5,000 per hour of sustained breach (&gt;30 consecutive minutes). Capped at INR 50,000/month.</p> <p><b>&gt;5 seconds P95:</b> P3 fault; capacity review within 5 business days; INR 10,000 per hour of sustained breach.</p> <p><b>&gt;10 seconds for &gt;1 hour:</b> Escalated to P2; additional P2 resolution penalties apply per SLA-06/SLA-08.</p>

### 3.4 Category D — Cybersecurity

#### SLA-10 | SIEM P1 Alert MTTR [Category D | WP-1(06) Security Stack + WP-4 O&M]

<b>Definition</b>	Mean Time to Respond by the CSOC to P1-priority SIEM alerts: ransomware indicators, unauthorised access to NCCC/RCCC, critical cloud security events, CERT-In notifiable incidents.
<b>Target</b>	< 15 minutes MTTR from SIEM alert generation to first CSOC containment/investigation action.
<b>Penalty</b>	0.5% of monthly OPEX per hour of cumulative P1 SIEM response delay in any month. IHMCL CISO escalation within 30 minutes of breach detection.

	Capped at 10% of monthly OPEX. ≥3 P1 SIEM MTTR breaches in a month: mandatory CSOC audit within 30 days.
--	--

**SLA-11 | CERT-In Mandatory Reporting** [Category D | WP-4 O&M + WP-5(02)]

<b>Definition</b>	Timely filing of notifiable cyber incidents with CERT-In per Section 70B of IT Act 2000 and CERT-In Directions dated 28 April 2022. IHMCL must be notified simultaneously.
<b>Target</b>	≤ 6 hours from CSOC confirmation of notifiable incident.
<b>Penalty</b>	<p><b>INR 5,00,000 per unreported or late-reported incident.</b></p> <p>P1 contract breach; IHMCL Director and Legal team notified immediately.</p> <p>IA bears full liability for any regulatory penalty imposed by MeitY or CERT-In for late reporting.</p> <p><b>≥2 failures in any 12-month period: potential Event of Default (Section 7.1).</b></p>

### 3.5 Category E — External Integrations

**SLA-12 | Government Integration Uptime** [Category E | WP-1(03-04) + WP-4 O&M]

<b>Definition</b>	Monthly availability of all mandatory external Government system integrations. Minimum 10 integrations: VAHAN, SARATHI, FASTag/NETC, e-Challan, Police systems, eCourts, State ICCCs, Rajmargyatra, CCTNS, Gati Shakti. Availability = IA API gateway can successfully exchange data within latency SLA.
<b>Target</b>	≥ 99% of scheduled operating hours per integration per month. API P95 response < 2 seconds per call.
<b>Measurement</b>	API gateway health monitoring at 5-minute intervals per endpoint. Per-integration availability dashboard accessible to IHMCL.
<b>Penalty</b>	P2 fault per integration not meeting 99% target. INR 5,000 per hour per integration endpoint beyond SLA. Capped at INR 50,000 per integration per month. Escalation to IHMCL if single integration unavailable >4 continuous hours. Total cap: 10% of monthly OPEX across all integrations.

<b>Note — Third-Party Downtime</b>	Downtime attributable solely to external Government system being offline (confirmed via system owner/official status page) is EXCLUDED from IA SLA. IA must document and report. IA has 30 days to adapt to API changes by external system.
------------------------------------	---

### 3.6 Category F — Disaster Recovery

#### SLA-13 | Disaster Recovery — RTO [Category F | WP-4(04) Annual DR Test + WP-4 O&M]

<b>Definition</b>	Recovery Time Objective: maximum elapsed time from declaration of complete DC failure to full ATMS platform restoration from DR site, including IHMCL operator confirmation of normal operations.
<b>Target</b>	<b>RTO &lt; 2 hours</b> from DC failure declaration. <b>⚠ DISCREPANCY FLAGGED — see Section 9.1</b>
<b>Measurement</b>	Validated through Annual DR Test (Q4). In real DC failure: IA NOC logs failure timestamp, DR activation timestamp, and IHMCL confirmation timestamp — reported to IHMCL within 24 hours.
<b>Penalty</b>	Annual DR Test Fail (RTO >2 hrs): Remediation Plan within 30 days; P1 Director escalation. Real DR event: P1 fault; 0.5% monthly OPEX per hour beyond 2-hour RTO. Cap: 10% monthly OPEX per event. 2 consecutive Annual DR Test failures: Performance Security invocation; potential Event of Default.

#### SLA-14 | Disaster Recovery — RPO [Category F | WP-4(04) Annual DR Test + WP-4 O&M]

<b>Definition</b>	Recovery Point Objective: maximum data loss permissible on full DC failure. Measured as time difference between last successful DC→DR data sync and moment of DC failure.
<b>Target</b>	<b>RPO &lt; 4 hours</b> from declared DC failure point. <b>⚠ DISCREPANCY FLAGGED — see Section 9.1</b>
<b>Penalty</b>	Annual DR Test Fail: Remediation Plan within 30 days; P1 escalation. Real event RPO breach: data loss assessment within 24 hours; potential regulatory breach notification if enforcement data lost. Financial: 0.5% monthly OPEX per 30 minutes of RPO exceedance. 2 consecutive Annual DR Test RPO failures: Performance Security invocation; Event of Default.

**SLA-15 | Annual DR Test Result** [Category F | WP-4(04) — One per O&M Year]

<b>Definition</b>	Outcome of mandatory annual full DC→DR failover simulation conducted in Q4 of each O&M year. PASS requires both RTO < 2 hours AND RPO < 4 hours.
<b>Target</b>	Annual DR Test Result: PASS (both thresholds met).
<b>Test Scope</b>	Full DC failure simulation; DR activation; NCCC restoration; data integrity validation; IHMCL operator sign-off on normal operations from DR. Witnessed by IHMCL Technical Director + independent observer + IA DR Test Manager.
<b>Penalty — Test Fail</b>	<p><b>INR 5,00,000 per Annual DR Test failure.</b></p> <p>Remediation Plan mandatory within 30 days.</p> <p>P1 escalation to Director level.</p> <p>Re-test mandatory within 60 days at IA's own cost.</p> <p><b>2 consecutive failures: Performance Security invocation (Clause 5.3); potential Event of Default (Section 7.1).</b></p>
<b>WP-4 Payment Link</b>	WP4-04 (Annual DR Test) unit rate is paid only upon test completion with signed report (RTO/RPO certificate per payment term 4.4). A FAIL does not prevent payment of WP4-04, but the INR 5,00,000 penalty is deducted from the subsequent quarterly OPEX invoice.

**3.7 Category G — Compliance & Governance****SLA-16 | Security Patch Deployment** [Category G | WP-4 O&M + WP-5(02/03)]

<b>Target</b>	100% of Critical CVEs (CVSS ≥9.0) patched within 72 hours of NVD/CERT-In disclosure. High CVEs (CVSS 7.0–8.9): patched within 14 days. Medium CVEs (CVSS 4.0–6.9): patched within 30 days.
<b>Vulnerability Log</b>	IA maintains live Vulnerability and Patch Management Log (updated within 4 hours of Critical CVE disclosure). IHMCL has read-only access at all times.
<b>Penalty</b>	<p><b>Critical CVE not patched within 72 hrs:</b> P1 fault; CERT-In notification; IHMCL Director escalation. INR 1,00,000 per day per unpatched Critical CVE beyond 72-hour window.</p> <p><b>High CVE not patched within 14 days:</b> INR 25,000 per day per unpatched High CVE.</p>

	<b>Critical CVE unpatched beyond 7 days:</b> Potential Event of Default (Section 7.1).
--	--

**SLA-17 | Annual Operator Training Compliance** [Category G | WP-5(01) Training]

<b>Target</b>	100% of all active NCCC/RCCC/LCCC operators to complete annual refresher training by 31 March of each O&M year.
<b>Evidence</b>	Signed attendance register or e-learning completion certificate per operator. Q1 Training Compliance Report submitted to IHMCL by 5 April each year.
<b>Penalty</b>	<p><b>&lt;100% but ≥90% by 31 March:</b> Training Compliance Escalation; remediation plan required.</p> <p><b>&lt;90% by 31 March:</b> INR 10,000 per non-compliant operator per week of delay beyond 31 March.</p> <p><b>&lt;90% by 30 April:</b> Contractual default if not remediated within further 60 days. Potential Event of Default (Section 7.1).</p>
<b>WP-5 Payment Link</b>	WP5-01 training unit rate paid per programme delivery and IHMCL Learning Manager sign-off (payment term 5.1). Non-compliance penalties deducted from subsequent WP-4 quarterly invoice — NOT from WP-5 programme payment.



#### 4. O&M Fault Categories — Definitions and Financial Penalties

The Fault Priority Framework governs every incident, defect, and enhancement request throughout the 10-year contract. Classification determines the SLA clock, financial penalty regime, and escalation path. Correct classification is the IA's responsibility — IHMCL may reclassify at any time.

Priority	Definition Summary	Response SLA	Resolution SLA	Financial Penalty	Escalation Path
<b>P1 CRITICAL</b>	Platform/national service down; >20% LCCCs offline; major cyber incident; enforcement pipeline fully down; DC failure + DR not activated within RTO; SIEM confirmed breach	<b>15 min</b>	<b>4 hrs</b>	0.5% monthly OPEX per hr beyond SLA (response + resolution). Cap: 10% monthly OPEX.	Director + War-room; CERT-In if cyber; IHMCL CEO if unresolved >2 hrs
<b>P2 HIGH</b>	Single RCCC down; >5% LCCCs offline; enforcement degraded; GIS unavailable; AI engine down; DR replication lag >15 min	<b>30 min</b>	<b>8 hrs</b>	0.25% OPEX/4-hr block + INR 5K/30-min response delay. Cap: 10% monthly OPEX.	O&M Manager + IHMCL Senior Manager; IHMCL Technical Director if >4 hrs unresolved
<b>P3 MEDIUM</b>	Single LCCC down; AI degraded; integration intermittent; data latency 3–10s; SIEM medium alert	<b>2 hrs</b>	<b>24 hrs</b>	0.1% OPEX per day beyond SLA. Cap: 10% monthly OPEX. Escalates to	Field Manager + Site Representative; weekly performance report

Priority	Definition Summary	Response SLA	Resolution SLA	Financial Penalty	Escalation Path
				P2 if open >5 business days.	
P4 LOW	Non-critical software defect; cosmetic UI issue; report formatting error; minor widget failure; non-critical configuration adjustment	4 hrs (acknowledge)	5 business days (or next release)	No penalty ≤30 days. INR 2,000/day if open >30 days. Cap: 1% monthly OPEX. Reclassified to P3 if open >60 days.	Defect log; monthly review; PM escalation if >30 days
P5 ENHANCEMENT	New feature; config change; data model extension; AI model retrain (ad-hoc); new corridor integration; new external system integration	5 business days (scoping estimate)	Per agreed CSO schedule	No penalty within CSO schedule. INR 5,000/day if scoping estimate not provided within 5 days. Delivery delays per CSO milestone terms.	Change Request process; Project Change Board if disputed; CSO required before commencement

**P1 — CRITICAL** Platform / National Service Down — Immediate Response Required

Response SLA	Resolution SLA	Financial Penalty
--------------	----------------	-------------------

15 minutes	4 hours	0.5% of monthly OPEX per hour (or part thereof) of delay beyond the 4-hour resolution SLA.
<b>Definition</b>	<p>A P1 — Critical incident is any fault or failure that renders the National ATMS Platform wholly or substantially inoperable, causes a complete loss of situational awareness at the NCCC or multiple RCCCs, poses an immediate risk to life (active emergency response disabled), results in total enforcement pipeline failure, or constitutes a critical cybersecurity breach requiring immediate containment.</p> <p>P1 incidents demand immediate, uninterrupted attention from the IA's most senior available engineers. All other non-critical tasks must be deprioritised until the P1 is resolved or downgraded.</p>	
<b>Trigger Examples (what constitutes this priority)</b>	<ol style="list-style-type: none"> <li>1. NCCC platform fully down — NCCC dashboard inaccessible to all operators.</li> <li>2. RCCC platform fully down affecting more than 1 RCCC simultaneously.</li> <li>3. More than 20% of DISC-certified commissioned LCCCs offline simultaneously.</li> <li>4. Major cyber incident — ransomware, data breach, unauthorised access to NCCC/RCCC, or any CERT-In notifiable incident.</li> <li>5. Enforcement pipeline completely down — no challans being generated or dispatched.</li> <li>6. DC (Primary Data Centre) full failure with DR not activated within the RTO window (i.e., recovery time objective breach — see SLA-17).</li> <li>7. Data lake ingestion completely failed — no field data reaching NCCC for &gt; 30 minutes.</li> <li>8. DR replication lag exceeding 60 minutes continuously (catastrophic RPO risk).</li> <li>9. SIEM P1 alert with confirmed malicious activity on platform infrastructure.</li> </ol>	
<b>Response SLA</b>	<p>15 minutes</p> <p>Response = SDA NOC engineer acknowledges IMS ticket, assigns named engineer, and posts initial assessment. Clock starts at IMS ticket creation timestamp.</p>	

<b>Resolution SLA</b>	<p>4 hours</p> <p>Resolution = full platform restoration confirmed by automated health checks + IHMCL operator sign-off + preliminary RCA posted in IMS ticket. Full RCA document within 48 hours of resolution.</p>
<b>Financial Penalty</b>	<p><b>0.5% of monthly OPEX per hour (or part thereof) of delay beyond the 4-hour resolution SLA.</b></p> <p><b>Example: P1 resolved at 7 hours = 3 hours beyond SLA = <math>3 \times 0.5\%</math> = 1.5% deduction.</b></p> <p><b>Response SLA breach (acknowledgement &gt; 15 minutes): additional 0.5% of monthly OPEX per hour of response delay.</b></p> <p><b>Aggregate P1 penalty capped at 10% of monthly OPEX across all P1 incidents in the month.</b></p> <p><b>3 or more P1 incidents in any single month: mandatory Director-level performance review. 3 consecutive months with P1 incidents unresolved within SLA: Performance Security invocation per Clause 5.3.</b></p>
<b>Escalation Path</b>	<p>Immediate (T+0): IA NOC Manager + IHMCL Duty Officer notified automatically by IMS.</p> <p>T+15 min (if not acknowledged): Auto-escalation to IA Director of Operations.</p> <p>T+30 min: War-room convened — IA Senior Engineers + IHMCL Technical Director.</p> <p>T+2 hours (if unresolved): IHMCL CEO / Executive Director notified.</p> <p>Cyber incidents: CERT-In notified within 6 hours of detection (per SLA-15).</p> <p>War-room cadence: status update every 30 minutes until P1 resolved.</p>
<b>Additional Notes</b>	<p>Mandatory Root Cause Analysis (RCA) document due within 48 hours of P1 closure. RCA must identify: root cause, contributing factors, timeline of events, corrective actions taken, and preventive measures. IHMCL reviews and accepts or rejects RCA.</p>

	War-room activation is mandatory if P1 is not resolved within 2 hours. War-room includes: IA Incident Commander, IA Senior Engineer(s), IHMCL Technical Director, Cloud Architect (for DC1/DR1 issues), IHMCL CISO (for cyber incidents).
--	---

<b>P2 — HIGH</b> Significant Degradation — Response Within 30 Minutes		
<b>Response SLA</b> 30 minutes	<b>Resolution SLA</b> 8 hours	<b>Financial Penalty</b> 0.25% of monthly OPEX per 4-hour block of delay beyond the 8-hour resolution SLA.
<b>Definition</b>	<p>A P2 — High incident is any fault or failure that significantly degrades the ATMS platform's operational capability across one or more zones or functional domains, without causing a complete national platform outage. P2 incidents affect a significant number of operators or LCCC sites, impair critical functionality, or pose a risk of escalation to P1 if not resolved promptly.</p> <p>P2 incidents require senior engineer engagement and must be treated as time-critical, although normal platform operations continue at a degraded level.</p>	
<b>Trigger Examples</b> (what constitutes this priority)	<ol style="list-style-type: none"> <li>1. Single RCCC fully down (one regional zone without its RCCC dashboard).</li> <li>2. More than 5% but not more than 20% of DISC-certified commissioned LCCCs offline simultaneously.</li> <li>3. Enforcement pipeline degraded — challans being generated but not dispatched, or dispatch rate reduced by more than 50%.</li> <li>4. GIS map layer unavailable at NCCC or RCCC level (operators cannot see corridor map).</li> <li>5. AI inference engine (VIDES / VSDS) fully down — no automated incident detection.</li> <li>6. DR replication lag exceeding 15 minutes but less than 60 minutes.</li> <li>7. More than 3 Government integration endpoints simultaneously unavailable.</li> <li>8. Platform data processing latency exceeding 10 seconds for more than 1 hour.</li> </ol>	

	9. SIEM P1 alert — potential (unconfirmed) security breach under investigation.
<b>Response SLA</b>	<p>30 minutes</p> <p>Response = SDA NOC engineer acknowledges IMS ticket and posts initial assessment. Clock starts at IMS ticket creation timestamp.</p>
<b>Resolution SLA</b>	<p>8 hours</p> <p>Resolution = affected component fully restored + data flow confirmed + IMS ticket closed with RCA summary. Full RCA document within 72 hours.</p>
<b>Financial Penalty</b>	<p><b>0.25% of monthly OPEX per 4-hour block of delay beyond the 8-hour resolution SLA.</b></p> <p><b>Example: P2 resolved at 18 hours = 10 hours beyond SLA = 2.5 blocks × 0.25% = 0.625% deduction.</b></p> <p><b>Response SLA breach (acknowledgement &gt; 30 minutes): INR 5,000 per 30-minute delay block.</b></p> <p><b>Aggregate P2 penalty capped at 5% of monthly OPEX across all P2 incidents in the month.</b></p> <p><b>5 or more P2 incidents in any single month: mandatory O&amp;M Manager + IHMCL Senior Manager performance review. Persistent P2 breaches may be escalated to P1 treatment.</b></p>
<b>Escalation Path</b>	<p>Immediate (T+0): SDA O&amp;M Manager notified automatically by IMS.</p> <p>T+20 min (if not acknowledged): Auto-escalation to IA Senior Operations Engineer.</p> <p>T+1 hour (if unresolved): IHMCL Senior Manager + IHMCL Cloud Team notified.</p> <p>T+4 hours (if unresolved): IA Director of Operations informed; enhanced monitoring.</p> <p>T+6 hours (if unresolved): IHMCL Technical Director informed; 2-hour escalation to P1 risk.</p> <p>Zone-specific RCC issues: IHMCL Regional Manager for affected zone informed.</p>

	Cyber (unconfirmed breach): IA CISO + IHMCL CISO engaged in parallel.
<b>Additional Notes</b>	<p>RCA summary required within 72 hours of P2 closure.</p> <p>If a P2 incident is not resolved within 6 hours, IHMCL must be notified of an estimated resolution time. If resolution is expected to exceed 8 hours (SLA breach), the IA must provide a written holding note to IHMCL with the revised estimated resolution time and actions being taken.</p> <p>A P2 incident may be escalated to P1 if: (a) it affects more than 20% LCCs; (b) a confirmed security breach is identified; (c) it persists beyond 8 hours.</p>

<b>P3 — MEDIUM</b> Limited Degradation — Response Within 2 Hours		
<b>Response SLA</b> 2 hours	<b>Resolution SLA</b> 24 hours	<b>Financial Penalty</b> 0.1% of monthly OPEX per day of delay beyond the 24-hour resolution SLA.
<b>Definition</b>	<p>A P3 — Medium incident is a fault or issue that causes limited degradation of ATMS platform performance or functionality, affects a small number of users or LCCC sites, or results in a non-critical service being impaired. Overall platform availability and core national operations continue without significant disruption.</p> <p>P3 incidents are managed within normal operational procedures and do not require senior management escalation unless they persist beyond the resolution SLA.</p>	
<b>Trigger Examples</b> (what constitutes this priority)	<ol style="list-style-type: none"> <li>1. Single LCCC down (one corridor offline — all others operational).</li> <li>2. AI inference engine (VIDES / VSDS) partially degraded — detection rate reduced but not zero (below 90% accuracy but above 85%).</li> <li>3. Government API integration intermittent for one endpoint (brief outages, &lt; 1 hour).</li> <li>4. Data processing latency between 3–10 seconds (above SLA but below P2 threshold).</li> <li>5. Non-critical dashboard widget or map layer failure (core platform unaffected).</li> </ol>	

	6. SIEM medium-priority alert requiring investigation (no confirmed breach).
<b>Response SLA</b>	<p>2 hours</p> <p>Response = SDA field / platform team acknowledges and confirms receipt of P3 ticket. Clock starts at IMS ticket creation timestamp.</p>
<b>Resolution SLA</b>	<p>24 hours</p> <p>Resolution = affected functionality restored + issue root cause identified + IMS ticket closed. Post-incident note within 5 business days.</p>
<b>Financial Penalty</b>	<p><b>0.1% of monthly OPEX per day of delay beyond the 24-hour resolution SLA.</b></p> <p><b>Example: P3 resolved at 50 hours = 26 hours beyond SLA (1.08 days) = 0.1% deduction.</b></p> <p><b>No financial penalty for response SLA breach, but escalation is triggered.</b></p> <p><b>Aggregate P3 penalty capped at 3% of monthly OPEX across all P3 incidents in the month.</b></p> <p><b>P3 incidents open for more than 5 business days without resolution: auto-escalated to P2 treatment for penalty purposes.</b></p>
<b>Escalation Path</b>	<p>T+0: IA Field Manager / Platform Engineer assigned in IMS.</p> <p>T+2 hours (if not responded): IA O&amp;M Manager notified.</p> <p>T+12 hours (if unresolved): IHMCL Site Representative / Zone Manager informed.</p> <p>T+24 hours (SLA breach): IA O&amp;M Manager + IHMCL Site Representative review call.</p> <p>T+5 business days (if still open): escalated to P2 for penalty purposes; weekly performance report flagged.</p> <p>Reported in Monthly SLA Performance Report with full list of P3 incidents, resolution times, and trend analysis.</p>



<b>Additional Notes</b>	<p>Brief incident note required within 5 business days of P3 closure. No formal RCA required unless the same P3 incident recurs more than 3 times in a 60-day period (in which case a root cause investigation is mandated).</p> <p>P3 incidents that have been open for more than 5 business days must be highlighted in the weekly NOC status report and the monthly SLA report.</p>
-------------------------	--

<b>P4 — LOW</b> Non-Critical — Normal Service Delivery Timeline		
<b>Response SLA</b> <b>4 hours</b> <b>(acknowledgement and logging in defect tracker)</b>	<b>Resolution SLA</b> <b>5 business days</b> <b>(or next scheduled maintenance release, whichever is earlier)</b>	<b>Financial Penalty</b> <b>No financial penalty for P4 incidents resolved within 5 business days.</b>
<b>Definition</b>	<p>A P4 — Low incident is a non-critical software defect, cosmetic issue, minor functional impairment, or non-urgent operational request that does not affect platform availability, core operational capability, or any SLA-critical function. The platform continues to operate fully for all critical operations.</p> <p>P4 items are managed through the standard defect log and resolved within the normal software maintenance cycle.</p>	
<b>Trigger Examples (what constitutes this priority)</b>	<ol style="list-style-type: none"> <li>1. Cosmetic user interface defect (display, formatting, colour, layout) that does not affect functionality.</li> <li>2. Report formatting error — data correct but layout or visual presentation incorrect.</li> <li>3. Minor dashboard widget failure (non-critical widget, core platform fully operational).</li> <li>4. Non-critical cloud monitoring alert (no performance impact confirmed).</li> <li>5. Minor documentation error in operator-facing help text or tooltips.</li> <li>6. Non-urgent configuration adjustment request (does not affect live operations).</li> </ol>	

	<p>7. Performance issue affecting a non-critical report or data export function (core monitoring and enforcement unaffected).</p> <p>8. Intermittent minor display refresh delay on secondary dashboards.</p> <p>9. Non-critical software defect identified in a feature not currently in active use.</p>
<b>Response SLA</b>	<p>4 hours (acknowledgement and logging in defect tracker)</p> <p>Response = SDA team logs defect in defect tracking system and assigns to relevant developer / operations stream.</p>
<b>Resolution SLA</b>	<p>5 business days (or next scheduled maintenance release, whichever is earlier)</p> <p>Resolution = defect fixed and deployed to production + IHMCL sign-off on fix. Defect log updated. No RCA required unless issue recurs 3+ times.</p>
<b>Financial Penalty</b>	<p><b>No financial penalty for P4 incidents resolved within 5 business days.</b></p> <p><b>If a P4 remains unresolved for more than 30 consecutive calendar days:</b> <b>INR 2,000 per day beyond 30 days, until resolved.</b></p> <p><b>If 10 or more P4 items remain open simultaneously for more than 30 days:</b> <b>the aggregate is treated as a systemic quality failure — O&amp;M Manager + IHMCL PM review required. Potential reclassification to P3 if patterns indicate a deeper technical issue.</b></p> <p><b>Aggregate P4 penalty capped at 1% of monthly OPEX.</b></p>
<b>Escalation Path</b>	<p>T+0: SDA developer / platform operations team logs in defect tracker.</p> <p>T+4 hours (acknowledgement): IHMCL notified via defect tracker (read-only access).</p> <p>T+5 business days (SLA expiry): flagged in monthly defect report for IHMCL PM review.</p>

	<p>T+30 days (if still open): IA O&amp;M Manager + IHMCL PM escalation call; root cause note required.</p> <p>All P4 items reviewed in monthly performance review meeting between IA PM and IHMCL PM.</p> <p>P4 items not resolved within 60 days are reclassified to P3.</p>
<b>Additional Notes</b>	<p>P4 items are batched into the regular software maintenance release cycle (monthly or quarterly minor release). IHMCL approves the release schedule.</p> <p>IA maintains a live defect log (read-only access for IHMCL) showing all open P4 items, their age, assigned engineer, and target release. The defect log is reviewed in the monthly performance review meeting.</p>

<b>P5 — ENHANCEMENT</b> New Feature / Change Request — Change Request Process		
<b>Response SLA</b> 5 business days (initial scoping estimate provided to IHMCL)	<b>Resolution SLA</b> Per agreed Change Request schedule (agreed in the signed CSO)	<b>Financial Penalty</b> No financial penalty if P5 work is delivered within the agreed CSO schedule.
<b>Definition</b>	<p>A P5 — Enhancement is any request for new functionality, platform configuration change, data model extension, AI model update, training delivery, new corridor or integration onboarding, or any other work that goes beyond the baseline contracted scope of work but does not constitute a defect or failure. P5 items are not faults — they are improvement or growth requests.</p> <p>P5 requests are processed through the formal Change Request (CR) process. No P5 work shall be commenced without a signed Change of Scope Order (CSO) from IHMCL, unless the request falls within the annual DEST enhancement retainer scope (WP-2).</p>	
<b>Trigger Examples</b> (what constitutes this priority)	<ol style="list-style-type: none"> <li>1. New feature or capability not included in the original Volume 2 scope.</li> <li>2. Platform configuration change affecting system behaviour (e.g., threshold adjustments, alert routing rule changes, new operator role definitions).</li> </ol>	

	<p>3. Data model extension — new data fields, new data types, new integration data streams.</p> <p>4. AI model retrain or new AI model deployment (scheduled biannual retraining is baseline O&amp;M; ad-hoc retraining triggered by accuracy event is P5 if outside retrain schedule).</p> <p>5. Training delivery — new training programme design or delivery for additional operators.</p> <p>6. New corridor integration — onboarding a new LCCC or corridor not in the original deployment schedule (WP3-06 applies; CSO required).</p> <p>7. New external system integration beyond the 7 baseline integrations.</p> <p>8. New report or dashboard design requested by IHMCL.</p> <p>9. Minor platform customisation for a specific zone or RCCC.</p>
<b>Response SLA</b>	<p>5 business days (initial scoping estimate provided to IHMCL)</p> <p>Response = IA project team acknowledges Change Request and provides an initial scoping estimate. Clock starts at CR receipt.</p>
<b>Resolution SLA</b>	<p>Per agreed Change Request schedule (agreed in the signed CSO)</p> <p>Resolution = feature / change delivered per agreed Change Request schedule + IHMCL User Acceptance Test (UAT) sign-off.</p>
<b>Financial Penalty</b>	<p><b>No financial penalty if P5 work is delivered within the agreed CSO schedule.</b></p> <p><b>If P5 delivery is delayed beyond the agreed CSO schedule: Penalty as specified in the CSO milestone payment terms (derived from the Financial Bid rate card).</b></p> <p><b>If IA fails to provide an initial scoping estimate within 5 business days of receiving a Change Request: INR 5,000 per day of delay.</b></p> <p><b>P5 items within the WP-2 DEST retainer scope (annual enhancement backlog, Years 6–10) are subject to the quarterly enhancement backlog meeting schedule agreed with IHMCL. No</b></p>

	<b>separate CSO is required for DEST-scope enhancements, but IHMCL Product Owner sign-off is required before development commences.</b>
<b>Escalation Path</b>	<p>CR receipt: IA Project Manager acknowledges and logs CR in the Change Management register.</p> <p>T+5 business days: IA submits scoping estimate (effort, cost, timeline) to IHMCL PM.</p> <p>IHMCL reviews estimate within 10 business days; issues CSO or returns with queries.</p> <p>Upon CSO signature: IA mobilises resources; IHMCL PM + IA PM manage delivery.</p> <p>Monthly CR Status Report: all open P5 items with status, milestone dates, and risks.</p> <p>Escalation to Project Change Board if: (a) scope is disputed; (b) cost estimate is challenged; (c) delivery timeline cannot be agreed within 20 business days.</p> <p>Project Change Board: IHMCL Technical Director + IA Programme Director.</p>
<b>Additional Notes</b>	<p>The Change Request process is governed by Clause 4.8 of this Agreement (Change of Scope — Payment Procedure).</p> <p>WP-2 DEST scope (Years 6–10): enhancements within the annual DEST retainer are prioritised in the quarterly backlog meeting between IHMCL Product Owner and IA DEST Lead. No CSO required for DEST-scope items, but all items must be logged in the enhancement backlog register.</p> <p>P5 items shall not be mixed with P1–P4 incidents in the IMS. P5 requests are managed in the Change Management register (separate from the Incident Management System).</p>

## 5. RESOURCE PENALTY FRAMEWORK — RATES AND TRIGGERS

All penalty rates in this section are applied against the monthly pro-rata OPEX value for the applicable WP and period. "Monthly OPEX" refers to one-third of the applicable quarterly payment rate (pro-rated per active instances per the DSC formula in Volume 4A). Penalties are cumulative and accrue daily or weekly as specified.

### 5.1 Tier 1 — Critical Role Vacancy Penalty

**Critical roles cannot be left vacant for more than 7 calendar days without IHMCL-approved named replacement in pipeline. Extended vacancies in Critical roles trigger escalating financial penalties and escalation obligations independent of SLA metrics.**

Vacancy Duration	Penalty Rate (per vacant Critical FTE per day)	Escalation Required	Additional Obligation
Days 1–7 (Transition Grace Period)	<b>No financial penalty</b> — grace period applies, provided IA has notified IHMCL within 5 business days and proposed a named replacement.	Written notice to IHMCL within 5 business days of vacancy.	Interim coverage plan submitted to IHMCL. Replacement must have equivalent or higher qualifications.
Days 8–30	<b>INR 7,500 per day</b> per vacant Critical FTE.	IA O&M Manager + IHMCL Technical Director notified.	Weekly status update on replacement progress. Interim cover plan must be in place and evidenced.
Days 31–60	<b>INR 15,000 per day</b> per vacant Critical FTE.	IA Programme Director + IHMCL Senior Director notified.	Show-cause notice issued. IA must demonstrate active recruitment and provide evidence. Remediation deadline set.
<b>Days 61+ (CRITICAL BREACH)</b>	<b>INR 25,000 per day</b> per vacant Critical FTE + potential withholding of quarterly OPEX payment.	<b>Formal Performance Notice issued. Potential invocation of Performance Security.</b>	If any Critical role remains vacant beyond 90 days: constitutes a material breach. IHMCL may invoke default remedies per Volume 3, Clause 7. Capped at 5% of monthly OPEX per vacancy.

Vacancy Duration	Penalty Rate (per vacant Critical FTE per day)	Escalation Required	Additional Obligation
Monthly cap — Tier 1	<b>Maximum 3% of monthly pro-rata OPEX per vacant Critical FTE per month. Aggregate cap across all Critical vacancies: 10% of monthly OPEX.</b>		

## 5.2 Tier 2 — Standard Role Shortfall Penalty

Standard role shortfall penalties are based on the percentage of FTE shortfall relative to the contracted total for that role group and period. Shortfalls are measured weekly. "Shortfall FTEs" = Contracted FTEs – Deployed FTEs for the same role.

Shortfall Level	Condition	Penalty Rate	Escalation
Level 0 — Within tolerance	Deployed FTEs $\geq$ 90% of contracted FTEs for the role	No penalty. Monthly report note required if shortfall persists >2 weeks.	None
Level 1 — Minor shortfall (10–25% below contracted)	Deployed FTEs = 75–89% of contracted FTEs for the role	INR 3,500 per missing FTE per week of shortfall.	IHMCL PM notified. Remediation within 30 days.
Level 2 — Significant shortfall (25–50% below contracted)	Deployed FTEs = 50–74% of contracted FTEs for the role	INR 7,000 per missing FTE per week of shortfall. + Monthly compliance report flag.	IA O&M Manager + IHMCL Senior Manager review call within 10 business days.
Level 3 — Severe shortfall (>50% below contracted)	Deployed FTEs < 50% of contracted FTEs for the role	INR 12,000 per missing FTE per week of shortfall. Payment hold risk.	Director-level escalation. Show-cause notice within 5 business days. Remediation plan required within 14 days.
Monthly cap — Tier 2	<b>Maximum 3% of monthly pro-rata OPEX per role group in shortfall per month. Aggregate cap across all Standard role shortfalls: 10% of monthly OPEX.</b>		

### 5.3 Tier 3 — LCCC Field Coverage Ratio Penalty

LCCC Field Technical Engineers are penalised based on the coverage ratio (Active LCCCs per deployed engineer) rather than a fixed headcount. This is because the number of active LCCCs changes throughout the contract as WP-3 deployment scales up.

Coverage Breach Level	Condition	Penalty	Escalation / Additional Obligation
Level 0 — Compliant	Deployed engineers $\geq$ contracted minimum (8 / 13 / 12 per period). Coverage ratio within contracted threshold.	No penalty.	None.
Level 1 — Minor (1–2 FTEs below required)	1–2 engineers below contracted minimum (e.g., 6–7 deployed vs. 8 required in Yrs 2–3).	INR 4,000 per missing LCCC engineer per week. Remediation within 30 days.	IHMCL notified. Monthly report flag. IA to provide recruitment/deployment plan within 14 days.
Level 2 — Significant (3+ FTEs below required)	3+ engineers below contracted minimum (e.g., $\leq 5$ deployed vs. 8 required in Yrs 2–3).	INR 8,000 per missing LCCC engineer per week. Plus: if LCCC online rate SLA-04 is simultaneously breached, both penalty streams apply independently.	Director-level escalation. Show-cause notice. Emergency deployment plan required within 7 days.
Level 3 — Coverage ratio exceeds 1:75	Deployed engineers $\times$ contracted max LCCCs per engineer $> 1.75\times$ threshold (e.g., each deployed engineer is covering 75+ active LCCCs).	INR 12,000 per engineer-week of coverage breach + P2 fault raised in IMS (linking to SLA-04).	Mandatory IHMCL Senior Manager review. Tied to LCCC online rate (SLA-04) penalties — dual penalty stream.
<b>Monthly cap — Tier 3</b>	<b>Maximum 5% of monthly pro-rata OPEX for LCCC coverage shortfall penalties per month. This cap is independent of and additive to SLA-04 online rate penalties.</b>		



## 6. WP-2 ENHANCEMENT TEAM — MAN-MONTH DELIVERY PENALTY

WP-2 is a retainer-based engagement. The contracted man-months per year per role represent the minimum delivery obligation. Penalties apply if the IA fails to deliver the contracted man-months in any given quarter.

### 6.1 Measurement Method

- Man-months are measured per role per calendar quarter (contracted annual MM ÷ 4 = contracted quarterly MM per role).
- The IA submits a Quarterly Team Deployment Report showing actual man-months delivered per role.
- IHMCL may request timesheet evidence, access logs, or deliverable attribution evidence to validate man-month claims.
- Quarterly man-month shortfall = Contracted Quarterly MM – Delivered Quarterly MM per role.

### 6.2 WP-2 Man-Month Shortfall Penalty Rates

Shortfall Level	Condition (% of contracted quarterly MM delivered)	Penalty	Additional Obligation
Level 0 — Compliant	≥ 90% of contracted quarterly man-months delivered for all roles in aggregate.	No penalty.	Quarterly deliverables accepted per Volume 4A WP-2 payment conditions.
Level 1 — Minor shortfall (10–20%)	80–89% of contracted quarterly MMs delivered in aggregate.	Proportional deduction from quarterly retainer: (Shortfall MM ÷ Contracted MM) × 50% × Quarterly Retainer Value.	IHMCL PM notified. Shortfall to be recovered in the following quarter (carry-forward allowed once).
Level 2 — Significant shortfall (20–40%)	60–79% of contracted quarterly MMs delivered.	Proportional deduction: (Shortfall MM ÷ Contracted MM) × 75% × Quarterly Retainer Value.	IHMCL PM + IA Programme Director review call. Recovery plan submitted within 14 days.
Level 3 — Severe shortfall (>40%)	< 60% of contracted quarterly MMs delivered.	Full proportional deduction: (Shortfall MM ÷ Contracted MM) × 100% × Quarterly Retainer Value. No carry-forward.	Director-level escalation. Formal performance notice. Potential payment hold on WP-2 quarterly retainer.

Shortfall Level	Condition (% of contracted quarterly MM delivered)	Penalty	Additional Obligation
Critical role (Solution Architect) not delivering contracted MMs in quarter	Any quarter in which Solution Architect man-months are < 75% of contracted.	Additional flat deduction: INR 50,000 per quarter in which Solution Architect is under-delivered, in addition to Level 1–3 proportional deduction.	Same as Tier 1 Critical Role Vacancy above (Section 4.1), if the under-delivery is due to vacancy.

**WP-2 Payment Link:** Quarterly retainer payment (Volume 4A, Section 6.2) is conditional on: (a) no critical unresolved defects from prior quarter; (b) quarterly deliverables accepted; (c) team deployment confirmation provided. Man-month shortfall penalties are deducted from the same quarterly invoice. Aggregate WP-2 resource penalty cap: 20% of WP-2 quarterly retainer per quarter.

## 7. WP-3 DEPLOYMENT TEAM — RESOURCE AVAILABILITY PENALTY

WP-3 staffing is critical to meeting corridor deployment milestones. Resource shortfalls in WP-3 have a direct downstream impact on WP-3 milestone achievement and WP-4 O&M SLA activation. Penalties under this section apply in addition to any milestone delay penalties under WP-3.

### 7.1 Measurement Method

- WP-3 team deployment is measured monthly via the Monthly Resource Deployment Report.
- Man-months are tracked per role per calendar quarter
- Corridor SAT pace is monitored by IHMCL. If the IA is behind on corridor commissioning targets, IHMCL may request evidence that the deployment team is adequately staffed.

### 7.2 WP-3 Man-Month Shortfall Penalty Rates

Shortfall Level	Condition	Penalty Rate	Milestone Link
Level 0	≥ 90% of contracted quarterly MMs delivered for all roles.	No penalty.	No impact on WP-3 milestone payment.
Level 1 (10–20% shortfall)	80–89% of contracted quarterly MMs.	INR 3,000 per shortfall man-month below 90% threshold.	Corridor onboarding pace review by IHMCL.
Level 2 (20–40% shortfall)	60–79% of contracted quarterly MMs.	INR 6,000 per shortfall man-month.	Deployment Plan review meeting with IHMCL within 14 days. Risk of milestone delay.
Level 3 (>40% shortfall)	< 60% of contracted quarterly MMs.	INR 10,000 per shortfall man-month + potential payment hold on WP-3 per-corridor payment.	Director-level escalation. Formal Performance Notice. IHMCL may direct IA to engage additional deployment resources at IA's cost.
Critical Role — Architect Vacancy	Deployment / Integration Architect absent >7 days without approved replacement.	Same as Tier 1 Critical Role Vacancy penalty (Section 4.1): INR 7,500/day (Day 8–30), INR 15,000/day (Day	Corridor onboarding may be halted pending Architect deployment. WP-3 milestones placed at risk.

Shortfall Level	Condition	Penalty Rate	Milestone Link
		31–60), INR 25,000/day (Day 61+).	

---

## 8. DEPLOYMENT VERIFICATION AND REPORTING

---

### 8.1 Monthly Resource Deployment Report

**Due:** Within 5 business days of each calendar month-end, submitted alongside the Monthly SLA Performance Report.

**Contents required:**

- **WP-4 Headcount Table:** For each role: contracted FTEs, deployed FTEs, names of deployed persons, location (NCCC/RCCC/LCCC/remote), days present vs. absent.
- **WP-2 Man-Month Delivery:** Quarterly progress against contracted man-months per role. Cumulative delivery YTD.
- **WP-3 Man-Month Delivery:** Same as WP-2. Plus per-corridor deployment pipeline status.
- **Vacancies declared:** Any role that was vacant for any period in the month: name of departing person, date of departure, days vacant, replacement status, proposed replacement name and expected start date.
- **Unauthorized substitutions self-declared:** Any role change not pre-approved by IHMCL. Self-declaration does not waive the penalty but IHMCL may consider a reduced flat deduction for proactive disclosure.
- **LCCC Coverage Ratio:** Current deployed engineers, current active LCCCs per DSC, coverage ratio, and variance from contracted ratio.
- **Qualifications verification:** For any new deployment in the month: CV and qualifications summary confirming compliance with Volume 2 minimum criteria.
- **Resource penalty self-assessment:** IA's own calculation of applicable resource penalties for the month, consistent with this schedule.

### 8.2 IHMCL Audit Rights

- IHMCL may, at any time and without advance notice, request: timesheets, access logs, employment records, or project management tool records to verify headcount claims.
- If a discrepancy is found between the declared deployment and actual deployment, IHMCL may impose a penalty of INR 2,00,000 per misrepresented person per month of misrepresentation, in addition to the applicable resource penalty.
- IHMCL may engage a third-party verifier to audit the IA's resource deployment at the IA's cost if material misrepresentation is suspected.

## 9. Penalty Calculation — Worked Examples

### 9.1 P1 Penalty Calculation

If a P1 incident (e.g., NCCC platform down) is logged at 09:00 and the Contractor does not begin remediation until 09:45, the response SLA of 15 minutes has been breached by 30 minutes. Additionally, if full resolution is achieved at 15:00 (6 hours total), the resolution SLA of 4 hours has been breached by 2 hours.

Breach Type	Hours in Breach	Penalty @ 0.5%/hr
Response SLA Breach (30 min = 0.5 hr)	0.5 hrs	$0.5 \times 0.5\% \times \text{Monthly Value}$
Resolution SLA Breach (2 hrs beyond 4-hr target)	2 hrs	$2 \times 0.5\% \times \text{Monthly Value}$
<b>TOTAL DEDUCTION</b>	<b>2.5 hrs</b>	<b>1.25% of Monthly Contract Value</b>

### 9.2 Uptime Penalty Calculation

Monthly uptime is measured in minutes. For a 30-day month (43,200 total minutes), the minimum uptime at 99.5% is 42,984 minutes. Any unplanned downtime that causes uptime to fall below this threshold triggers a SLA deduction applied to the monthly invoice.

### 9.3 Penalty Cap

Unless otherwise specified in Volume 2 of the O&M Agreement, total monthly SLA deductions are capped at 20% of the monthly contract value in any single calendar month. Breach of the cap does not extinguish the Employer's right to raise a formal contractual default notice.

---

## 10. Measurement, Reporting and Governance

---

### 10.1 Monthly SLA Report

The SDA shall submit a Monthly SLA Performance Report to the Employer within 5 business days of the end of each calendar month. The report shall include actual vs. target performance for each SLA parameter, a log of all incidents by priority, RCA summaries for all P1 and P2 incidents, and a calculation of any applicable deductions.

### 10.2 Real-Time Monitoring

All SLA parameters covered by platform availability, LCCC online rate, data latency, and integration uptime shall be monitored in real time via the ATMS Operations Dashboard, accessible to authorised Employer representatives at all times. Employer representatives may independently log incidents in the IMS.

### 10.3 Dispute Resolution

If the SDA disputes the Employer's calculation of an SLA breach or penalty, the SDA must raise a written Notice of Dispute within 10 business days of receipt of the SLA deduction notice. The dispute shall be referred to the O&M Oversight Committee and, if unresolved within 30 days, to the dispute resolution mechanism set out in the main O&M Agreement.

### 10.4 Exclusions

The following conditions shall not count as downtime or SLA breaches, provided the Contractor has complied with applicable notice requirements:

- Pre-approved scheduled maintenance windows (minimum 72 hours' advance notice)
- Force majeure events as defined in the O&M Agreement
- Failures caused directly by third-party government system outages (e.g., VAHAN, SARATHI) where the Contractor has no contractual control
- Failures caused by Employer-directed changes implemented without Change Request approval

**APPENDIX D – ABBREVIATIONS AND GLOSSARY (ADDENDUM)**

Term	Definition
<b>ASVS</b>	Application Security Verification Standard (OWASP)
<b>AWS</b>	Automated Weather Station
<b>AZ</b>	Availability Zone (isolated data centre within a CSP region)
<b>CII</b>	Critical Information Infrastructure (NCIIPC classification)
<b>CIS</b>	Center for Internet Security (CIS Benchmarks for OS and cloud hardening)
<b>CSIRP</b>	Cybersecurity Incident Response Plan
<b>CSOC</b>	Cybersecurity Operations Centre (24x7 security monitoring team)
<b>CSP</b>	Cloud Service Provider
<b>CVE / CVSS</b>	Common Vulnerability and Exposure / Common Vulnerability Scoring System
<b>DAST</b>	Dynamic Application Security Testing
<b>DEST</b>	Development-cum-Enhancement Support Team (Section 34.2)
<b>EDR</b>	Endpoint Detection and Response (security software for endpoint protection)
<b>EPS</b>	Events Per Second (SIEM ingestion capacity metric)
<b>HIDS</b>	Host-based Intrusion Detection System
<b>IAST</b>	Interactive Application Security Testing
<b>IaC</b>	Infrastructure as Code (Terraform, Bicep, CloudFormation)
<b>ILT</b>	Instructor-Led Training
<b>IMD</b>	International Metreological Data
<b>KP</b>	Kilometre Post
<b>MEITY</b>	Ministry of Electronics and Information Technology, Government of India
<b>MSTG / MASVS</b>	Mobile Security Testing Guide / Mobile Application Security Verification Standard
<b>NMS</b>	Network Management System
<b>NVD</b>	National Vulnerability Database (US NIST)
<b>ODBC</b>	Open Database Communication



<b>PAM</b>	Privileged Access Management
<b>POI</b>	Point of Interest
<b>SBOM</b>	Software Bill of Materials
<b>SAST</b>	Static Application Security Testing
<b>SCORM</b>	Sharable Content Object Reference Model (e-learning standard)
<b>SSDLC</b>	Secure Software Development Lifecycle
<b>STRIDE</b>	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (threat modelling)
<b>TMCS</b>	Traffic Monitoring Camera System
<b>UEBA</b>	User and Entity Behaviour Analytics (ML-based SIEM capability)
<b>VAPT</b>	Vulnerability Assessment and Penetration Testing
<b>WORM</b>	Write Once Read Many (immutable storage policy for legal/compliance data)
<b>YoY</b>	Year-on-Year (annual growth projection)