



# **Guide for ensuring the deployment of Trust, Quality, Integrity, Security, and Sovereignty of TN-ITS data Concepts of data chain evaluation tools (update)**

Contribution from Sub-Working Group 4.2

Status: Final  
Version: 1.0  
Date: 10 March 2025

## **Legal disclaimer**

The sole responsibility for the content of this document lies with the authors. It does not necessarily reflect the opinion of the European Union. The European Commission is not responsible for any use that may be made of the information contained therein. All images are provided by the respective partners (unless otherwise noted) and are approved for reproduction in this publication.



This project has received funding from the European Commission's Directorate General for Transport and Mobility under Grant Agreement no. MOVE/B4/SUB/2020-123/SI2.85223

### Document information

<b>Project acronym</b>	NAPCORE
<b>Full project title</b>	National Access Point Coordination Organisation for Europe
<b>Grant Agreement No.</b>	MOVE/B4/SUB/2020-123/SI2.852232
<b>Activity no. and title</b>	4.2.4 TN-ITS enhancements concerning the data sharing supply chain
<b>Author(s)</b>	Rodolfo Da Silva - KIOS CoE, Cyprus
<b>Co-author(s)</b>	Madiha Shahzad - KIOS CoE, Cyprus Georgios Christou, Frank Daems - ERTICO
<b>Related to Milestone No.</b>	M 4.2.7
<b>External Milestone</b>	Yes

### Document history

Version	Date	created/ modified by	Comments
Draft	25.04.2024	Rodolfo Da Silva - KIOS CoE, Cyprus Georgios Christou - ERTICO	Draft (ToC) version
0.1	04.07.2024	Rodolfo Da Silva - KIOS CoE, Cyprus Madiha Shazad - KIOS CoE, Cyprus Barry Koloway - KIOS CoE, Cyprus Soteris Petrikkos - KIOS CoE, Cyprus Sara Guerra de Oliveira - UM, Slovenia Nele Dedene – Flemish government Frank Daems ERTICO Stephen T'Siobbel ERTICO Richard Rek – CEDA, Czech Republic Edwin 't Lam – WSP, Finland András Selmeczy – Közút, Hungary Biró Tamás – Közút, Hungary Massimiliano Masi – Autostrade, Italy	Initial version
0.11	08.08.2024	Rodolfo Da Silva - KIOS CoE, Cyprus	Clean version
0.2	12.08.2024	Rodolfo Da Silva - KIOS CoE, Cyprus Madiha Shazad - KIOS CoE, Cyprus Barry Koloway - KIOS CoE, Cyprus Soteris Petrikkos - KIOS CoE, Cyprus	Second version
0.3	10.02.2025	Rodolfo Da Silva - KIOS CoE, Cyprus Madiha Shazad - KIOS CoE, Cyprus Barry Koloway - KIOS CoE, Cyprus Soteris Petrikkos - KIOS CoE, Cyprus Richard Rek – CEDA, Czech Republic Edwin 't Lam – WSP, Finland Frank Daems ERTICO	Third version
1.0	10.03.2025	Rodolfo Da Silva - KIOS CoE, Cyprus Madiha Shazad - KIOS CoE, Cyprus Soteris Petrikkos - KIOS CoE, Cyprus	Final version
1.0	16.04.2025	Hannah Walther	Edit of Template, final Version after SCOM Approval



**Document status:**

<input type="checkbox"/>	To be revised by partners involved in the preparation of the document
<input type="checkbox"/>	For review/ approval by the Core Alignment Team and Peer Reviewers
<input type="checkbox"/>	For approval by the NAPCORE Steering Committee
<input checked="" type="checkbox"/>	Final
<input type="checkbox"/>	Updated/revised final version (e.g. when a second version of Milestone is published)

**Abstract**

This report is part of Task 4.2.4 from the NAPCORE project, which focuses on TN-ITS enhancements of the data sharing supply chain by incorporating and enhancing various data aspects of TN-ITS related data. The main objective of this report is to identify, ensure, and document the concepts of trust, quality, integrity, security, and sovereignty within the TN-ITS data chain. The report outlines:

1. Relevant standards, regulations/directives, and projects/initiatives that serve as the basis for the analyses/suggestions of this milestone.
2. Improvement of the TN-ITS data-chain presentation (concerning the previous milestone 4.2.6) regarding data aspects, data stages, roles/stakeholders, and feedback loop.
3. Application guide of all the above-mentioned factors of the TN-ITS data chain demonstrated through a speed limit use case.
4. Suggestions and directives for an optimal TN-ITS data-chain system.
5. Presentation of potential tools, methods, and best practices to complement the optimal TN-ITS data-chain system.

**Note:** This document represents the final version of the deliverable 4.2.7, building upon the draft presented in Milestone M4.2.6, titled, “TN-ITS Inventory on requirements related to trust, quality, integrity, security and sovereignty of data”. Milestone M4.2.7 is inherently linked to and dependent on the work conducted in M4.2.6, serving as a continuation. **Consequently, substantial information detailed in M4.2.6 is not reiterated in this report.**

## Abbreviations

Abbreviation	Meaning
AAA	Authentication, Authorisation, and Accounting
ABB	Architecture Building Blocks
ADAS	Advanced Driver Assistance Systems
ADASIS	ADAS Interface Specifications
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threats
BP	Business Prospect
CA	Cooperation Agreement
CC	Common Criteria
CCAM	Cooperative, Connected, and Automated Mobility
CEF	Connecting Europe Facility
CEN	European Committee for Standardisation
CIA triad	Confidentiality, Integrity, Availability triad
C-ITS	Cooperative Intelligent Transport Systems
CPOC	C-ITS Point of Contact
CSIRT	Computer Security Incident Response Team
CWA	CEN Workshop Agreement
DATEX II	DATA EXchange between traffic and travel information centers
DCAT	Data CATALOGue vocabulary
DCAT-AP	DCAT Vocabulary Application Profile for Data Portals in Europe
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DoS	Denial of Service
DR	Delegated Regulation
DSC	Dataspace Connector
EC	European Commission
EDIC	European Digital Infrastructure Consortium
EIF	European Interoperability Framework
EMDS	European Mobility Data Space
ENISA	European Union Agency for Cybersecurity
ERTICO ITS Europe	European Road-transport Telematics Implementation Coordination Organisation
ETSC	European Transport Safety Council
EU	European Union
EUCC	European Union Common Criteria
EU-EIP D4.1	Determining Quality of European ITS Services
EU-EIP	EU ITS Platform
Euro NCAP	European New Car Assessment Programme
Euro RAP	European Road Assessment Programme
FAIR	Findable, Accessible, Interoperable, Reusable



Abbreviation	Meaning
GDF	Geographic Document Files
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IBB	Implementation Building Blocks
ICT	Information and Communications Technology systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISA	Intelligent Speed Assistance
ISG	Innovation and Scaling Group
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ITS	Intelligent Transport Systems
JSON	JavaScript Object Notation
LC	Level of Implementation complexity (technical)
LI	Level of Importance
LLF	Level of Organisational/Legal Feasibility Complexity
MaaS	Mobility as a Service
MDS	Mobility Data Space
METR	Management of Electronic Traffic Regulations
MITRE ATT&CK	MITRE (Corporation) Adversarial Tactics, Techniques, and Common Knowledge
mobilityDCAT-AP	Mobility extension for the DCAT application profile for data portals in Europe
MS	Member States
NAP	National Access Point
NAPCORE	National Access Point Coordination Organisation for Europe
NAPCORE M4.2.6	Milestone “Requirements on trust, quality, integrity and security”
NAPCORE M4.2.7	Milestone “Guide on ensuring potential deployment of trust, quality, integrity, and security of data established. Concepts of data evaluation tools (update)”
NAPCORE T4.2.4	SWG 4.2 (TN-ITS) /T4.2.4 (TN-ITS Enhancements concerning the data sharing supply chain)
NIS 2 Directive	Security of Network and Information Systems Directive
OEM	Original Equipment Manufacturer
OpenID	Authentication Protocol for signing Users into client applications
OWASP	Open Worldwide Application Security Project
PDI	Physical and Digital Infrastructure
PKI	Public key Infrastructure
QF	Quality Framework
R&I	Research and Innovation
RDF	Resource Description Framework
REST	REpresentational State Transfer
RTTI	Real-Time Traffic Information
SAML	Security Assertion Markup Language
SENSORIS	SENSOR Interface Specification



Abbreviation	Meaning
SHACL	SHApes Constraint Language
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SOAP	Simple Object Access Protocol
SOCRATES 2.0	System of Coordinated Roadside and Automotive Services for Traffic Efficiency and Safety 2.0
SRTI	Delegated Regulation for Road Safety-related Universal Traffic Information
STRIDE threat model	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege threat model
sWG	sub-Working Group
SWOT	Strengths, Weaknesses, Opportunities, Threats
TCP	Traffic Circulation Plan
TEN-T	Trans-European Transport Network
TISA	Traveller Information Services Association
TLT	Threat Landscape for the Transport Sector
TLS/SSL	Transport Layer Security/Secure Sockets Layer
TM2.0	Traffic Management 2.0
TN-ITS	Transport Network – Intelligent Transport Systems: <a href="http://www.tn-its.eu">www.tn-its.eu</a>
TN-ITS GO	TN-ITS sub-project
WG	Working Group
XML	eXtensible Markup Language format

## Table of Contents

<b>1. Introduction.....</b>	<b>10</b>
1.1. Overarching objectives of Task 4.2.4 .....	10
1.2. Scope of the report M4.2.7 .....	12
1.3. Relation with NAPCORE WG4 sub-working groups .....	12
1.4. Methodology .....	14
<b>2. Desk Research – an update.....</b>	<b>16</b>
2.1. Data sharing related aspects .....	16
2.1.1. Trust (on Stakeholder) .....	16
2.1.2. Quality (of Data) .....	17
2.1.3. Integrity (of Data) .....	17
2.1.4. Security (on data & exchange) .....	17
2.1.5. Sovereignty (of the data) .....	17
2.2. Relevant standards, regulations/directives, and projects/initiatives .....	17
2.2.1. Standards Additional/New Standards .....	17
2.2.2. Regulations / Directives .....	21
2.2.3. Projects/initiatives (non-exhaustive).....	23
2.2.3.1. METR (updates).....	26
2.2.3.2. TISA - RTTI 5-Star Quality Rating.....	27
2.2.3.3. TISA Guideline ‘Digital Map Quality Assessment Framework for In-Vehicle ISA Systems’	28
2.2.3.4. TM2.0 (updates).....	28
2.2.3.5. POLIS RTTI Task Force .....	29
2.2.4. Relevant NAPCORE activities (updates) .....	29
2.2.5. Mobility Data Space (updates) .....	32
2.2.5.1. Benefits of TN-ITS in the MDS.....	34
2.2.5.2. TN-ITS Use Cases .....	35
2.2.5.3. Challenges and Future Opportunities.....	37
<b>3. TN-ITS Data Chain .....</b>	<b>39</b>
3.1. TN-ITS Stakeholders and Their Harmonized Roles.....	39
3.1.1. Role-Based Stakeholder Grouping.....	40
3.2. Data chain stages .....	41
3.3. Feedback Loop.....	41
3.3.1. Introduction to the Feedback Loop .....	42



3.3.2.	Legal context.....	42
3.3.3.	Types of Feedback Loop .....	43
3.3.4.	Feedback Loop Possible Scenarios .....	44
3.3.5.	Challenges and Limitations.....	51
3.4.	TN-ITS Data-chain Updated Diagram .....	51
<b>4.</b>	<b>Critical evaluation of TN-ITS data chain processes.....</b>	<b>54</b>
4.1.	Data chain stages and data aspects analysis.....	54
4.2.	Mapping Stakeholder Responsibilities to Data Aspects.....	54
4.3.	Data aspects overlapping analysis .....	57
<b>5.</b>	<b>Optimal TN-ITS Data-Chain Framework .....</b>	<b>61</b>
5.1.	Potential vulnerabilities, attacks, and countermeasures (Update) .....	61
5.1.1.	Targeted Countermeasures: Addressing Vulnerabilities.....	61
5.1.2.	Vulnerabilities Impact Assessment and Critical Data Aspects .....	63
5.1.3.	Identifying Key Stakeholders for Countermeasure Implementation .....	65
5.1.3.1.	Analysis of Security and Integrity-Related Identified Vulnerabilities .....	66
5.2.	TN-ITS security and integrity .....	67
5.2.1.	Approach for ensuring suitable security and integrity mechanism .....	68
5.3.	TN-ITS trust.....	69
5.3.1.	Technical Approach for Ensuring Suitable Trust Mechanism.....	69
5.3.1.1.	Organisational Approach for Ensuring Suitable Trust Mechanism.....	71
5.3.2.	Levels of Cooperation .....	71
5.3.3.	Key Considerations for Cooperation Levels.....	72
5.3.4.	TN-ITS Levels of Trust .....	73
5.3.5.	Approach for Ensuring Trust.....	75
5.3.6.	Trust Recommendations .....	77
5.4.	TN-ITS quality .....	78
5.4.1.	Approach for ensuring suitable data quality mechanism .....	78
5.4.2.	Definition of Quality Criteria .....	78
5.4.3.	Levels of Quality .....	81
5.4.4.	TN-ITS data chain quality levels analysis .....	83
5.4.5.	Minimum Level Requirement.....	84
5.4.6.	Monitoring Quality and Evaluation Methods.....	84
5.4.7.	Quality Recommendations .....	85
5.5.	TN-ITS sovereignty.....	86

- 5.5.1. Approach for Ensuring a Suitable Data Sovereignty Mechanism..... 86
- 5.5.2. Implications of Data Sovereignty..... 87
- 6. Data chain evaluation tools and best practices for optimal TN-ITS system..... 90**
  - 6.1. Requirements for data evaluation tools ..... 90
  - 6.2. Categories of Data Evaluation Tools ..... 90
  - 6.3. Identification of data evaluation tools..... 91
  - 6.4. Data evaluation tools criteria ..... 95
    - 6.4.1. Level of impact/importance..... 95
    - 6.4.2. Level of implementation complexity (technical) ..... 96
    - 6.4.3. Level of organizational & legal complexity ..... 96
    - 6.4.4. Level of business prospect ..... 97
    - 6.4.5. Weighted average of all criteria..... 97
  - 6.5. Concepts and best practices for TN-ITS data evaluation tools ..... 98
    - 6.5.1. Standardized metadata schema / DCAT-AP ..... 99
      - 6.5.1.1. mobilityDCAT-AP ..... 101
    - 6.5.2. Feedback loop tools..... 103
- 7. Use Case Analysis: Speed Limit.....106**
  - 7.1. Motivation for Selecting the Speed Limit Use Case ..... 106
  - 7.2. Requirements and Expectations ..... 106
  - 7.3. Analysis Procedures..... 107
  - 7.4. Data Chain stage and Stakeholders analysis ..... 108
    - 7.4.1. Data holders – speed limit analysis ..... 108
    - 7.4.2. Data Users – speed limit analysis ..... 109
    - 7.4.3. Access Point – speed limit analysis..... 111
    - 7.4.4. Service Providers – speed limit analysis ..... 112
    - 7.4.5. End-Users – speed limit analysis ..... 113
  - 7.5. Analysis Reflections and Strategic Insights ..... 114
- 8. Conclusions and recommendations .....116**
  - 8.1. Key contributions of M4.2.7 ..... 116
    - 8.1.1. TN-ITS and DATEX II Alignment SWOT Analysis..... 117
  - 8.2. Deployment plan/roadmap..... 123
  - 8.3. Potential Recommendations..... 123
  - 8.4. Future steps..... 125
- 9. Annexes.....126**



## Introduction

In today's increasingly data-driven world, the effective management of static transport network data is critical to ensuring robust and reliable infrastructure services. Road safety and efficiency require highly updated digital maps. Changes in static road attributes are exchanged using the Transport Network - Intelligent Transport Systems (TN-ITS) CEN TS (Technical Specification) 17268. The TN-ITS framework establishes a pivotal data chain to facilitate not only data exchange but also establish connections between different stakeholders, including public authorities and private sector partners such as map providers. As the complexity of Intelligent Transport Systems (ITS) and Cooperative Intelligent Transport Systems (C-ITS) services continues to grow, along with the adoption of the EU Intelligent Speed Assistance (ISA) Regulation, it becomes essential to address key aspects of static or map related data such as data trust, quality, integrity, security, and sovereignty.

The work on the National Access Point Coordination Organisation for Europe (NAPCORE) project deliverable/milestone 4.2.7, from the sub-Working Group (SWG) 4.2 - TN-ITS, titled “Guide for ensuring the deployment of Trust, Quality, Integrity, Security and Sovereignty of TN-ITS data Concepts of data chain evaluation tools (update)” aims to provide comprehensive insights and practical steps for ensuring data quality, establishing trust among stakeholders, and security to ensure data integrity and sovereignty. The task consists of the following subtasks:

1. Continuation of close collaboration with the NAPCORE Member States (MS) technical expert teams and the TN-ITS community.
2. Organization of monthly meetings (4.2.4 task meetings) with MS representatives to allocate tasks and responsibilities for the creation of the report (Milestone 4.2.7).
3. Establishment of expert groups focusing on specific data aspects (quality, trust, security, integrity, and sovereignty) and the feedback loop.
4. Addressing the significant challenge of integrating all existing factors in the TN-ITS data chain with the diverse realities in each MS.
5. Provision of a comprehensive report that offers support and recommendations for all MS using/providing TN-ITS related data.

### 1.1. Overarching objectives of Task 4.2.4

TN-ITS is a standardized data-sharing framework driven by end-user needs, focused on the exchange of map attribute updates between road authorities and digital map service providers. Its primary goal is to address data priorities that fulfil the end-user needs for various mobility applications and services by providing digital maps that ensure up-to-date and accurate data. In the short term, TN-ITS aims to significantly support the implementation of ISA, and the adoption of the European ‘Vision Zero’ strategy<sup>1</sup>.

---

<sup>1</sup> European Climate, Infrastructure and Environment Executive Agency (CINEA), *EU Road Safety: Towards “Vision Zero”*, 2022 [https://ec.europa.eu/transport/themes/strategies/news/2019-06-19-vision-zero\\_en](https://ec.europa.eu/transport/themes/strategies/news/2019-06-19-vision-zero_en)



The main objective of TN-ITS is to ensure that public road authorities, the data hubs, create and make authoritative data available, with the highest quality possible, to meet the needs of the service providers for the benefit of the end-users. Achieving data availability, accessibility, and quality is based upon a joint effort and agreement between the public and the private sectors as per Real-Time Traffic Information (RTTI) Delegated Regulation (DR) 2022/670<sup>2</sup>. Building on the work completed in Milestone 4.2.6<sup>3</sup>, this document highlights the progress made in the context of the NAPCORE project, noting the completed and ongoing objectives of Task 4.2.4.

One of the primary objectives of Task 4.2.4, according to the Grant Agreement, was to build a foundation of trust and ensure quality, integrity, security, and sovereignty. A team of technical experts was established within the NAPCORE MS to research, make an inventory, and perform an assessment of data trust, quality, integrity, security, and sovereignty related items and mechanisms. Furthermore, the team assessed the complete end-to-end data chain of TN-ITS data for vulnerabilities, identifying and classifying potential vulnerabilities and suggesting countermeasures. Research, coupled with expert consultation, was conducted on the most optimal quality system that can be applied to TN-ITS services, based on inputs from the EU-EIP D4.1. “Determining Quality of European ITS Services”. The team also worked on a deployment approach for bidirectional TN-ITS data exchange, in the form of the so-called Feedback loop, considering the limitations and available resources of involved stakeholders.

Another objective of Task 4.2.4 was to develop a data quality assessment methodology. The research team focused on evaluating the implementations within the TN-ITS GO project, particularly related to the data and protocol structure, to develop a generic data quality assessment methodology that considers the aspects of the TN-ITS data space and relates data quality to RTTI. As part of the goal of aligning DATEX II with TN-ITS, Working Groups WG3 and WG4 have contributed with relevant information in meetings and workshops to ensure alignment and coherence within the NAPCORE project.

Finally, the third objective of Task 4.2.4 was to develop concepts and mechanisms for data quality evaluation and enrichment tools. Based on the previous objectives, the aim was to create a concept for data quality enrichment and assessment tools, while also leveraging existing tools such as those developed in the TN-ITS GO project, addressing their shortcomings. In M4.2.6, it was ensured that this Milestone would suggest possible combined approaches from different components and services, such as:

- Quality Criteria (Level of Services and Data Quality Criteria) listed from TN-ITS GO, EU ITS Platform (EU-EIP), and the latest 5-star rating proposed by the Traveller Information Services Association (TISA).
- Data aspects (Trust, Quality, Integrity, Security, and Sovereignty).
- The Feedback Loop tool - built upon the TN-ITS Data Chain Feedback loop diagram proposed in M4.2.6 and focused on refining key areas to efficiently illustrate the roles, stages, and feedback taking place in the data chain.

---

<sup>2</sup> European Commission, *Commission Delegated Regulation (EU) 2022/670*, pp. 1–2 (February 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0670>

<sup>3</sup> NAPCORE, *TN-ITS Inventory on requirements related to trust, quality, integrity, security and sovereignty of data*, August 2023, [https://www.napcore.eu/documents/M4.2.6Concepts\\_data\\_evaluation\\_tools.pdf](https://www.napcore.eu/documents/M4.2.6Concepts_data_evaluation_tools.pdf)



- Principles of models of cooperation from the Traffic Management 2.0 (TM2.0) project.

Furthermore, the team has also worked on defining and refining the data aspects, stakeholders and their or other roles, and identifying potential assessment tools and best practices to be used throughout the data chain stages.

### **1.2. Scope of the report M4.2.7**

This report aims to provide comprehensive insights and practical steps to enhance the TN-ITS data chain. The report can be divided into three main segments. The first part is an update of relevant activities and developments within the broader domain of ITS, the second part covers the TN-ITS data chain enhancements and critical evaluation, while the third part covers the methods and tools to incorporate and ensure quality, trust, security, integrity, and sovereignty within the TN-ITS data chain. Milestone M4.2.7 builds upon the foundation established in Milestone M4.2.6, serving as its continuation. Consequently, information previously covered in M4.2.6 will not be duplicated in this report. Instead, M4.2.7 focuses on providing updates and enhancements to the material presented in the previous report, M4.2.6. These improvements and updates are documented comprehensively in this milestone to ensure the progression and refinement of the work initiated in M4.2.6.

Since this work eludes on the data aspect topics, standards, and technologies currently under active research and deployment, an update of relevant activities is presented in this report in Chapter 2. It should be noted that the status updates of several relevant initiatives such as TISA, METR, and TM2.0 are documented. Within the NAPCORE project, the progress made by different WGs, pertinent to this task, are reported as well.

### **1.3. Relation with NAPCORE WG4 sub-working groups**

The WG4 aims to develop and enhance standards while aligning current EU actions with the enablement of harmonization activity. In this regard, it establishes coordination between different data standards approaches and defines a common roadmap for the following sub-working groups:

- SubWG 4.1: DATEX II
- SubWG 4.2: TN-ITS
- SubWG 4.3: Multimodal data
- SubWG 4.4: Metadata

The alignment challenge is addressed through a common task between all SWGs. The following are some explanations of the need for the existence of this relationship within the different sub-working groups.

#### **DATEX II**

On May 24, 2023, during the Lisbon EU ITS congress, DATEX II and the TN-ITS platform signed the Declaration of Lisbon<sup>4</sup>. This declaration marks a significant breakthrough as the two data standards commit to a merger, taking their collaboration to the next level. The action

---

<sup>4</sup> TN-ITS, *TN-ITS and DATEX II sign the Declaration of Lisbon at the ITS European Congress*, May 2023, <https://tn-its.eu/2023/05/tn-its-and-datex-ii-sign-the-declaration-of-lisbon-at-the-its-european-congress/>



encompasses various aspects, including a joint approach to data quality and data exchange service improvements.

A Cooperation Agreement (CA) between TN-ITS and DATEX II is being developed. This CA aims to strengthen a common position in the mobility data space with, among others, joint technical specification work and alignment on the unification of the related data standards and the establishment of a common approach.

SWG 4.1 (DATEX II) released a new version of its standard, version 3.5, on the 17th of June 2024<sup>5</sup>. The latest version did not take any steps in harmonizing the two standards, but it is expected that version 4, which is scheduled to be released in 2025, will address this and bring updates in JSON mapping and mapping with new modern serialization formats. Additionally, the DATEX II public repository was moved to GitHub along with a bug reporting.

The scope of this document remains focused on the TN-ITS data chain itself. However, we anticipate that the findings and results of this task will also benefit the DATEX II group and will have a direct effect. Furthermore, it should be noted that tasks from the SWG 4.1 DATEX II, such as Task 4.1.6 “Encoding and transfer”, where quality and trust concepts are considered, are working in close collaboration with this task. The Task 4.1.6 technical experts regularly collaborate during the Task 4.2.4 meetings and have contributed to the technical content of this report, ensuring high-level alignment. Since this merger was not envisioned at the beginning of the NAPCORE project, the relevant activities were not considered in the original project timeline. In the case of the NAPCORE project extension, the focus will be on continued collaboration towards technical alignment.

In the final part of this report, the plan for the alignment process between the two standards is presented, along with possible challenges that will need to be overcome in this process.

### **Multimodal data**

In the context of multimodality, the availability of high-quality trusted TN-ITS data can improve overall MaaS (Mobility as a Service) or public transport services decision-making, reduce congestion, and optimize travel, ultimately leading to more efficient and synchronized multimodal transport networks. High-quality digital maps with strong multimodal support are a key building block for realizing a true MaaS solution. An up-to-date static layer provides a reliable foundation that services can use to develop and integrate their solutions. With an emphasis on the activities currently undertaken by SWG4.3, there is no direct association or impact.

### **Metadata**

The alignment and closer collaboration between the TN-ITS and Metadata sub-working groups is essential, as the metadata schema mobilityDCAT-AP, developed under the Metadata sub-working group, stands out as one of the key tools highlighted in this report for significantly enhancing the existing data quality.

---

<sup>5</sup>DATEX II, *DATEX II Model*, <https://docs.datex2.eu/static/data/v3.5/umlmodel/html/index.htm> (last accessed December 2024)



### 1.4. Methodology

Addressing this task is challenging due to the complex interplay between trust, quality, integrity, security, and sovereignty of data within the TN-ITS data chain, which involves multiple actors and functionalities affecting each other. To approach this problem scientifically, a methodology comprising continuous and integrated stages was developed.

In the initial phase, the methodology builds upon the activities conducted in Milestone 4.2.6, with updates in the steps of desk research focused on critical data aspects such as trust, quality, integrity, security, and sovereignty, particularly within the transportation domain. This work establishes a solid foundation for formulating appropriate definitions and achieving a common understanding of these terms. The research involves a detailed inventory and the establishment of the relevance of the data aspects, utilizing relevant inputs from NAPCORE, the EU EIP, TN-ITS GO project, and TISA’s proposal for a 5-star rating system for data quality assessment. These efforts provide essential groundwork for the methodology, enabling the valuable expertise of the project participants to be leveraged.

Based on this groundwork, a description and critical evaluation of the TN-ITS data chain are conducted, highlighting potential vulnerabilities and challenges at each stage of the data chain. These activities are enhanced through workshops, which foster collaborative discussions and refinement of the analyses.

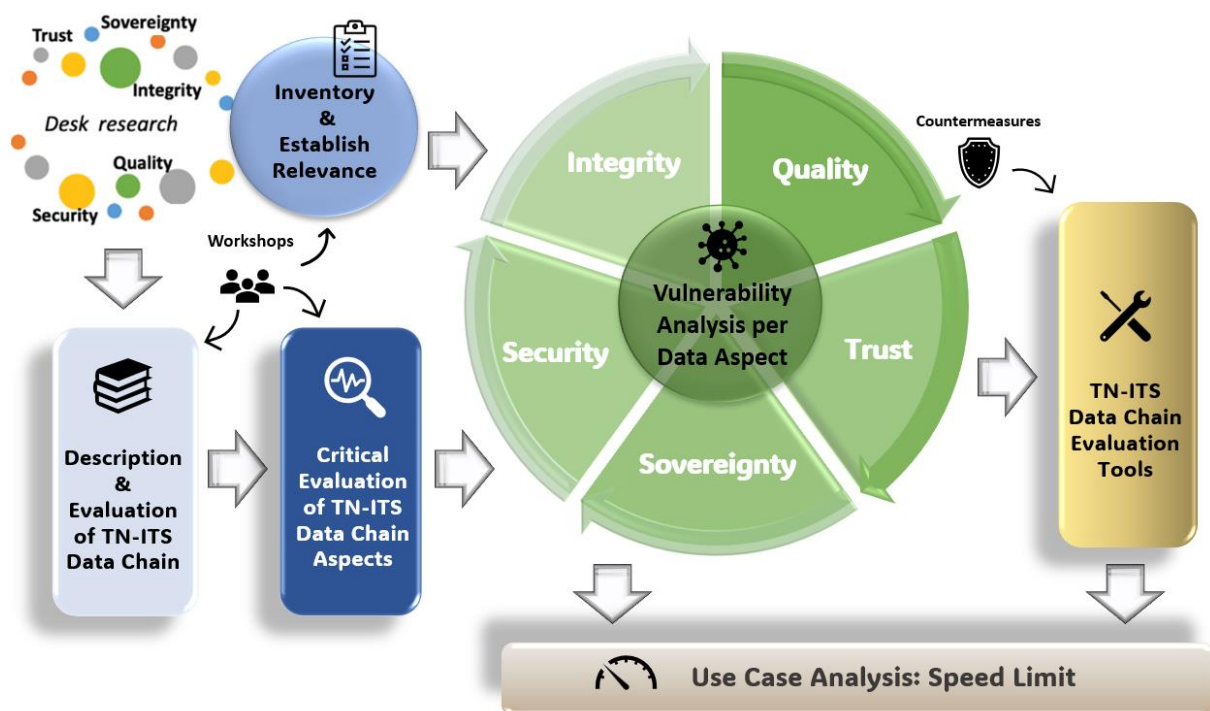


Figure 1 - Task 4.2.4 Methodology

The subsequent phase aims to propose an optimized TN-ITS data chain based on the identified critical data aspects. This phase includes updating the critical assessments of potential vulnerabilities and mitigation measures (countermeasures), some of which were identified in



the previous milestone. Moreover, potential evaluation tools will be suggested to enhance the TN-ITS data chain, with a focus on tools ensuring trust, quality, security, integrity, and sovereignty. All this information will be applied in a selected use case analysis focused on the relevant topic of speed limits.

## 2. Desk Research – an update

This chapter provides updates since the last report, building upon Milestone 4.2.6 of Task 4.2.4. It aims to track progress and highlight developments, ensuring consistency across milestones. By avoiding redundant information, there is a focus on presenting new insights and achievements.

**Note:** This chapter is not intended to replicate the detailed information presented in the previous milestone report, Milestone 4.2.6. Instead, the focus here is on providing relevant updates and new insights that have emerged since the last report. The objective is to highlight key developments, changes and enhancements that are significant for this current milestone. By focusing on these updates, we aim to ensure that the report remains concise and focused on the most critical information, allowing stakeholders to efficiently understand the progress and advancements made.

### 2.1. Data sharing related aspects

To facilitate a cohesive understanding, this section elucidates the definitions of data sharing related aspects proposed by the active members of Task 4.2.4, informed by their accrued experience throughout the task and the research conducted on these matters in the preceding Milestone 4.2.6.

The established definitions aim to offer concise and easily understandable descriptions accessible to all readers, regardless of their familiarity with the subject matter.

#### 2.1.1. Trust (on Stakeholder)

Definition agreed upon by members of Task 4.2.4:

“Trust within TN-ITS denotes the confidence TN-ITS stakeholders possess regarding the reliability and credibility of the TN-ITS data chain. This encompasses stakeholders' trust in maintaining consistent levels of data quality, integrity, and security while participating in the chain, all while preserving their sovereignty.”

The outcome of the workshop on Trust, along with expert discussions, distinguishes trust into two distinct forms. The first, termed Organizational Trust, is inspired by the confidence placed in people, institutions, and governance structures. It reflects the credibility, accountability, and ethical integrity of organizations in handling data. The second, referred to as Technical Trust, focuses on embedding and ensuring trustworthiness within data chain processes. This includes the security, reliability, and interoperability of data, systems, and technologies. Together, these two dimensions form a holistic approach to fostering trust in digital ITS ecosystems. This deliverable primarily considers the organisational trust aspect since technical trust requires deep dive into technical aspects of data.

The relationship between data quality, security, integrity, and sovereignty with data trust is inherently complex. These elements are deeply interdependent, and one cannot exist in isolation without the others, and each plays a critical role in reinforcing and enhancing the overall trustworthiness of data. Data quality ensures accuracy and reliability, security safeguards against unauthorized access and breaches, integrity preserves consistency and



authenticity, while sovereignty upholds control and compliance with legal frameworks. Their interplay is essential for establishing a robust foundation of trust in data ecosystems. A more in-depth discussion on this topic is presented in Chapter 4.

### 2.1.2. Quality (of Data)

Definition agreed upon by members of Task 4.2.4:

"Data quality, inspired by the EU-EIP data quality parameters, encompasses various quality criteria including reporting period, location accuracy, latency (content side), timeliness (start), classification correctness, event coverage, error rate, report coverage, and timeliness (update)."

### 2.1.3. Integrity (of Data)

Definition agreed upon by members of Task 4.2.4:

"Data integrity entails maintaining the consistency, reliability, and accuracy of data throughout its lifecycle, ensuring it remains uncorrupted, unaltered, and authentic during all stages of the TN-ITS data chain processes."

### 2.1.4. Security (on data & exchange)

Definition agreed upon by members of Task 4.2.4:

"Data security entails safeguarding data against unauthorized access, disclosure, alteration or destruction. This involves implementing measures and safeguards to uphold the confidentiality, integrity, availability, and secure exchange of data."

### 2.1.5. Sovereignty (of the data)

Definition agreed upon by members of Task 4.2.4:

"Data sovereignty is a legal concept encompassing the rights and control an entity holds over its data, dictating access, management, and usage permissions."

## 2.2. Relevant standards, regulations/directives, and projects/initiatives

The following sections will maintain a consistent structure, presenting the name of standards, regulations/directives, and projects/initiatives, along with general information and their relevance to this report (Milestone 4.2.7).

### 2.2.1. Standards Additional/New Standards

**Name:** ISO 21177:2024 (Intelligent Transport Systems – ITS station security services for secure session establishment and authentication between trusted devices).

**General Information:** This standard specifies Intelligent Transport System (ITS) station security services that ensure secure information exchanged between trusted devices. Such services include secure session establishment, authentication, confidentiality, and integrity aspects, which are essential for a solid and secure exchange of information. These security services are vital for various ITS applications and services, such as time-critical safety applications, automated driving, remote management of ITS stations, and infrastructure



related services, which eventually will enhance the trustworthiness and safety of the ITS network<sup>6</sup>.

**Relation with M4.2.7:** This standard represents one of the main references for the development of data aspects related to security, integrity, and trust within the TN-ITS data chain. The proposed optimal session for the TN-ITS Trust framework will be divided into an organizational level and a technical level, where ISO 21177:2024 will play a fundamental role, with the possible suggestion of implementing ITS station security services to enhance trustworthiness across the entire ecosystem.

**Name: ISO/IEC TR 24028:2020** (Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence).

**General Information:** This standard comprehensively examines factors pertinent to the trustworthiness of AI systems, encompassing the strategies for building trust in AI systems through transparency, explainability, and controllability mechanisms. Additionally, it includes the identification of engineering pitfalls and typically associated threats and risks inherent to AI systems, alongside potential mitigation techniques and methodologies. Furthermore, the document discusses approaches for evaluating and attaining the availability, resilience, reliability, accuracy, safety, security, and privacy of AI systems. By considering the recommendations outlined in ISO/IEC TR 24028:2020, developers and implementers of ITS systems can potentially enhance privacy protections while still harnessing the benefits and building trust towards TN-ITS<sup>7</sup>.

**Relation with M4.2.7:** ISO/IEC TR 24028:2020, which focuses on the trustworthiness of AI, is integrated into this report by guiding the potential incorporation of AI into various tools discussed. While no specific AI tool is introduced, the report ensures that all tools are designed with AI integration in mind, following the standard's principles of transparency, explainability, and controllability. This approach ensures that future AI adoption within the TN-ITS data chain will align with international trustworthiness standards, maintaining the system's integrity and reliability.

**Name: ISO 27001:2022** (Information security, cybersecurity, and privacy protection - Information security management systems).

**General Information:** The governance aspects for the cybersecurity of an organization are set by this standard. It defines an Information Security Management System (ISMS) by defining the rules and the practices that can be implemented using the guidance of ISO 27002:2022. The scope is defined on an organizational basis. ISO 27001 is the foundational standard for the C-ITS implementation and other national guidelines. Certification against ISO 27001 is recognized in Europe. ISO 27001 defines also internal audits. Security testing such as Penetration Testing on software and hardware is also provisioned by the application of ISO

<sup>6</sup> ISO, *ISO 21177:2024 (en) Intelligent transport systems – ITS station security services for secure session establishment and authentication between trusted devices*, 2024

<https://iss.isolutions.iso.org/obp/ui#iso:std:iso:21177:ed-2:v1:en>

<sup>7</sup> ISO, *ISO/IEC TR 24028:2020 (en) Information technology—Artificial intelligence—Overview of trustworthiness in artificial intelligence*, 2020, <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24028:ed-1:v1:en>.



27001. To attain the interoperability required by the NIS 2 directive (EU 2022/2555), the NAP security architecture should provide common guidance on a defined scope<sup>8</sup>.

**Relation with M4.2.7:** ISO 27001 is closely related to the report as it provides a framework for managing information security, which is a critical component of the TN-ITS data chain discussed in the report. The report focuses on ensuring the trust, quality, integrity, security, and sovereignty of TN-ITS data. ISO 27001 helps establish and maintain these security aspects by defining a structured approach to managing sensitive TN-ITS data and personal information so that it remains secure. This is particularly relevant for the TN-ITS system, where data integrity and security are essential to ensuring reliable and trustworthy data exchanges between stakeholders.

**Name: CWA 18125:2024.**

**General Information:** This is a CEN Workshop Agreement (CWA) developed by the European Committee for Standardization (CEN). This document aims to establish terminology, concepts, and mechanisms in the field of data exchange, with an emphasis on trusted data transactions. Those elements can serve as a foundation for developing standards that support trusted data transactions among stakeholders<sup>9</sup>. It provides a framework for creating trust in data transactions, ensuring that all stakeholders involved can rely on the data's integrity and security. The guidelines support interoperability between different systems and organizations, facilitating seamless data exchange across various platforms.

**Relation with M4.2.7:** CWA 18125:2024 is directly related to the "approach for ensuring a suitable trust mechanism" in the report. This section is divided into technical and organizational components. The standard is crucial in the technical part, where it provides guidelines to ensure that data exchanges within the TN-ITS data chain are secure and trustworthy, supporting both the integrity and reliability of the system.

**Name: ISO 13888-1:2020 (Information Security – Non-repudiation).**

**General Information:** Part 1 of this standard is related to non-repudiation in information security. As specified in the document, the non-repudiation services objective is to generate, gather, preserve, make available, and verify evidence about a particular event or action to resolve disputes related to the occurrence or non-occurrence of the event or action. This standard provides a model for non-repudiation services and the non-repudiation mechanisms using cryptographic techniques<sup>10</sup>. Part 1 is followed by two parts on mechanisms using symmetric techniques and mechanisms using asymmetric techniques.

**Relation with M4.2.7:** ISO 13888 is directly related to the "Non-Repudiation ABB" in the section "approach for ensuring a suitable security and integrity mechanism", as it provides the standards necessary for ensuring that actions such as data submission and delivery cannot be

<sup>8</sup> ISO, *ISO/IEC 27001:2022 (en) Information security, cybersecurity and privacy protection—Information security management systems—Requirements*, 2022, <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>

<sup>9</sup> NEN, *CWA 18125:2024 (en) Trusted Data Transaction*, July 2024, <https://www.nen.nl/en/cwa-18125-2024-en-326590>

<sup>10</sup> ISO, *ISO/IEC 13888-1:2020 (en) Information security—Non-repudiation—Part 1:General*, 2020, <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:13888:-1:ed-4:v1:en>



denied by either party. This enhances the security and integrity of TN-ITS data exchanges by ensuring reliable and verifiable data transactions.

**Name: ISO 20524** (Intelligent Transport Systems – Geographic Data Files (GDF 5.1)).

**General Information:** Replaces ISO 14825:2011 and provides the conceptual and logical data model and physical encoding formats for geographic databases that can be used in Intelligent Transport System (ITS) applications and services. The standard specifies the databases' potential content, such as data dictionaries for features, attributes, and relationships, how these contents should be depicted or represented, and how the information behind the data can be specified (metadata). The ISO 20524 consists of two parts, the first part focuses on ITS applications and services, with a particular emphasis on road and road related information, while the second part centers on cutting edge ITS application and services such as C-ITS, and automated driving systems with an emphasis on road, lane and relevant information on road and lane<sup>11</sup>.

**Relation with M4.2.7:** In the implementation of interoperability tools within the TN-ITS framework, such as those in the Syntactic Validation Category, it is essential to consider standards like ISO 20524. By aligning these tools with ISO 20524, the TN-ITS framework can enhance its ability to ensure that geographic data is not only syntactically correct but also interoperable across different platforms and frameworks. This alignment helps maintain high data quality and reliability, which are crucial for the successful integration of diverse ITS applications.

**Name: ISO/IEC 15408** (Information technology – Security techniques – Evaluation criteria for IT security).

**General Information:** This is an international standard that provides a comprehensive framework for evaluating the security properties of information technology products and systems. Commonly known as the Common Criteria (CC), this standard consists of three parts, each addressing different aspects of IT security evaluation:

- a) Introduction and general model - Outlines the foundational concepts and principles for evaluating IT security, establishing a common understanding and framework for security assessment.
- b) Security functional requirements - Defines the functional requirements for security features, ensuring that the IT products provide the necessary security functionalities to protect against various threats.
- c) Security assurance requirements - Specifies the assurance requirements, detailing the criteria for evaluating the confidence in the security features of IT products.

The EUCC (European Union Common Criteria) certification is the European implementation of this standard, allowing IT products to be evaluated and certified according to the rigorous standards of ISO/IEC 15408. This certification is recognized across the European Union,

---

<sup>11</sup> ISO, *ISO 20524-2:2020(en) Intelligent transport systems—Geographic Data Files (GDF) GDF5.1—Part2: Map data used in automated driving systems, Cooperative ITS, and multi-modal transport*, 2020, <https://www.iso.org/obp/ui/en/#iso:std:iso:20524:-2:ed-1:v1:en>



ensuring that certified products meet a specific level of security assurance, which is critical for high-security environments such as government and military applications<sup>12</sup>.

**Relation with M4.2.7:** ISO/IEC 15408, the Common Criteria, will be used as a tool in the security audits category within the TN-ITS framework ensuring that the TN-ITS infrastructure meets international security standards. This strengthens the security of the system, ensuring it is robust and reliable against potential threats.

### 2.2.2. Regulations / Directives

**Name: EU ITS Directive 2010/40/EU.**

**General Information:** The ITS Directive 2010/40/EU (consolidated version including amendments of Directive 2023/2661/EU) on the framework for the deployment of Intelligent Transport Systems in the field of road transport and interfaces with other modes of transport has been amended in 2023. The amendment aims to adapt to the emergence of new road mobility options, mobility apps, and connected and automated mobility. It proposes that certain crucial road, travel, and traffic data should be made available in digital format, such as speed limits, traffic circulation plans, or roadworks. It also ensures that essential safety-related services are made available for drivers along the TEN-T network<sup>13</sup>. Annex III of the Directive explains how data is categorised relating to the provision of road traffic information and navigation services, including speed limits and other variables such as access conditions for tunnels and bridges.

**Relation with M4.2.7:** The ITS Directive emphasizes the need for standardised digital formats for road and traffic data while ensuring interoperability and data consistency. By focusing on the trust, security, sovereignty, integrity, and quality of data aspects and providing tools and recommendations on how to optimise them, this milestone contributes to the successful deployment of ITS solutions as highlighted by the Directive.

**Name: Commission Delegated Regulation (EU) 2019/1789** supplementing Directive 2010/40/EU of the European Parliament and the Council concerning the deployment and operational use of cooperative intelligent transport systems.

**General Information:** The C-ITS certificate policy authority (Article 24), managed by the Commission until a dedicated entity is established, oversees the certificate policy and PKI authorization as outlined in Annex III. The trust list manager (Article 25), also temporarily managed by the Commission, is responsible for maintaining the European Certificate Trust List (ECTL) and reporting to the certificate policy authority. Additionally, the C-ITS point of contact (Article 26), managed by the Commission until further notice, handles communication with

<sup>12</sup>ISO, *ISO/IEC 15408-1:2022 (en) Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1: introduction and general model*, 2022

<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:15408:-1:ed-4:v1:en>

<sup>13</sup> European Parliament and Council. *Directive 2010/40/EU of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems, amended by Directive (EU) 2023/2661*. *Official Journal of the European Union*, L 207, August 2010, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02010L0040-20231220>



root certification authority managers and publishes the public key certificate of the trust list manager and the ECTL<sup>14</sup>.

**Relation with M4.2.7:** Focusing on Article 10a of the ITS Directive, the specifications for the EU C-ITS security credential management system are outlined, highlighting the need for duties for a C-ITS certificate policy authority, a C-ITS trust list manager and a C-ITS point of Contact. This is further expanded upon in this delegated regulation. Both legislative documents are important as they help understand how to set up a certificate policy for the TN-ITS Trust Architecture as well, utilising the TLM and ECTL specifications outlined in DR (EU) 2019/1789.

**Name: EU Regulation on the Provision of EU-wide Real-time Traffic Information Services (2022/670).**

**General Information:** The EU Regulation 2022/670, amending EU Regulation 2015/962, as its predecessor aims to improve the availability and quality of traffic information to enhance mobility and reduce congestion<sup>15</sup>.

**Relation with M4.2.7:** The RTTI DR is directly related to this milestone, especially with Articles 4 and 5 as they highlight requirements for accessibility, exchange, and re-use of data on infrastructure and regulations & restrictions, to be provided in DATEX II or TN-ITS format. Furthermore, the role of the feedback loop in the data chain that is analysed in-depth in this milestone is highlighted, with the two articles emphasising the need to ensure that any inaccuracies related to data should be flagged and resolved by data holders and data users.

**Name: NIS 2 Directive (Directive (EU) 2022/2555).**

**General Information:** The NIS 2 directive is an update of the original NIS directive implemented by the European Union. The NIS 2 directive aims to achieve a high common level of cybersecurity across the Union. The directive focuses on strengthening cybersecurity in member states by bolstering the resilience and incident response capabilities of critical sectors. To achieve this objective, this directive outlines various requirements, including but not limited to, the adoption of national cybersecurity strategies by Member States, the designation or establishment of competent authorities, cyber crisis management bodies, and computer security incident response teams (CSIRTs). In addition, it also regulates the implementation of cybersecurity risk-management measures and reporting obligations for critical entities, as well as rules and obligations on cybersecurity information sharing<sup>16</sup>.

**Relation with M4.2.7:** As this milestone pays great attention to security when it comes to data, the NIS2 Directive is directly related, helping to strengthen cybersecurity strategies and countermeasures for the data circulated through the TN-ITS data chain. Furthermore, this relation is further strengthened by the previously mentioned ISO 27001 standard.

<sup>14</sup> European Commission, *Commission Delegated Regulation (EU) 2019/1789/EU of 13 March 2019 supplementing Directive 2010/40/EU with regard to cooperative intelligent transport systems*, 2019, [https://eur-lex.europa.eu/resource.html?uri=cellar:9a2fe08f-4580-11e9-a8ed-01aa75ed71a1.0014.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:9a2fe08f-4580-11e9-a8ed-01aa75ed71a1.0014.02/DOC_1&format=PDF)

<sup>15</sup> European Commission, *Commission Delegated Regulation (EU) 2022/670*, (February 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0670>

<sup>16</sup> European Parliament and Council, *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, OJ L 333, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555>



**Name: Regulation (EU) No 2024/1679** of the European Parliament and of the Council of 11 December 2024 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU.

**General Information:** This Regulation (informally called the TEN-T Regulation) and its latest revisions of 18 March 2024 outlines the priorities for the development of the trans-European transport network and establishes guidelines for its development while identifying projects of common interest, like NAPCORE.<sup>17</sup>

**Relation with M4.2.7:** As TN-ITS contributes to the provision of the policy framework for transport network development in the EU, the main goal of the TEN-T Regulation through the TN-ITS data chain, it is important to consider its guidelines and impositions when relating to this milestone.

**Name:** EU Intelligent Speed Assistance (ISA) Regulation (Regulation (EU) 2019/2144).

**General Information:** The Intelligent Speed Assistance (ISA) regulation mandates that all new vehicles in the EU be equipped with ISA systems starting July 2022, with broader implementation across all new cars by July 2024. ISA systems aim to improve road safety by using data from digital maps, cameras, and vehicle sensors to provide drivers with real-time information on current speed limits and, in some cases, intervene to prevent speeding. This regulation aligns with the EU's Vision Zero strategy to reduce road fatalities and serious injuries to nearly zero by 2050. The ISA regulation underscores the importance of accurate, reliable, and timely data for ensuring system functionality and user trust.

**Relation with M4.2.7:** M4.2.7 supports the ISA regulation by enhancing the quality and reliability of digital map data through the TN-ITS data chain. The milestone provides tools and methodologies for evaluating data accuracy, completeness, and timeliness, which are critical for ISA compliance. By aligning with standards such as the TISA Digital Map Quality Assessment Framework (which will be discussed later in the milestone), M4.2.7 helps to ensure that the spatial and traffic regulation data needed for ISA systems are up to date and meet regulatory requirements. Furthermore, the milestone's focus on feedback loops allows for continuous improvements in data quality, directly supporting the successful deployment of ISA systems across Member States.

### 2.2.3. Projects/initiatives (non-exhaustive)

**Name: SENSORIS**

**General Information:** The [SENSORIS](#) project was initiated by automotive, mapping, and navigation companies, and its main goal was to enhance the quality and reliability of ITS data. SENSORIS focuses on the vehicle-to-cloud upload form and the cloud-to-cloud data exchange format, specifically for vehicle-based data and other data needed for mobility services. The cloud can be an intermediate server, aggregation server, or a service provider input gateway.

<sup>17</sup> European Parliament and Council, *Regulation (EU) 2024/1679 of 13 June 2024 on Union guidelines for the development of the trans-European transport network, amending Regulations (EU) 2021/1153 and (EU) No 913/2010 and repealing Regulation (EU) No 1315/2013*, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_202401679](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401679)



SENSORIS closes the loop between the vehicle's sensors, map, and connected services. In addition to attributes describing the in-vehicle status, the data specification covers observable and derived attribution of the world from various categories, including weather environment, road infrastructure, traffic regulation, traffic events and behaviour, and in-vehicle status. SENSORIS aims to enhance data quality and reliability by establishing standards of data formats, real-time data sharing, and improving interoperability of such systems<sup>18</sup>.

**Relation with M4.2.7:** The SENSORIS project is complementary to the TN-ITS data chain as it can provide real-time information of dynamic data from vehicles, providing more comprehensive information, as both are focused on the provision of standardised spatial real-time static information, with SENSORIS providing dynamic vehicle-based data and TN-ITS static data such as traffic signs and speed limits.

**Name: EURO NCAP:** The European New Car Assessment Programme

**General Information:** [Euro NCAP](#) has created a five-star safety rating system to help consumers evaluate and compare vehicles more easily, and to help them identify the safest choice for their needs. The safety rating is determined from vehicle tests, designed and carried out by Euro NCAP. Some cars have two different star ratings. One is based on a car fitted only with safety equipment reflecting the safety measures and features that the car provides. The second rating is based on the level and functionality of additional "safety pack features" that may be offered as an add-on option to consumers.

The number of stars reflects how well a car performs in these tests but is also influenced by what safety equipment the car manufacturer is offering to the market. There is no legal requirement for the car makers to conduct these tests and are purely voluntary. A car that only meets the minimum legal demands would not receive any stars. This means that if a car is rated poorly, it does not necessarily mean it is unsafe, but it is not as safe as competitors that are rated better.

The benchmark for vehicles encourages car makers to improve the quality of their technologies and cars, respectively. It influences customers' choices with a simple way of showing cars from an additional point of view. Therefore, the rating influences quality and reliability on the market<sup>19</sup>.

**Relation with M4.2.7:** Euro NCAP's five-star safety rating system laid the groundwork for the TISA star rating system used in traffic information services. TISA, through its RTTI (Real-Time Traffic Information) Task Force, promotes the development of accurate and timely traffic data standards, essential for road safety. Both Euro NCAP and the RTTI Task Force aim to enhance road safety—Euro NCAP focuses on vehicle design and safety features, while TISA, through RTTI, ensures that safety technologies are paired with real-time, standardized road and traffic data. Together, these standards help maximize the effectiveness of safety technologies in vehicles.

**Name: ETSC** (European Transport Safety Council)

**General Information:** [ETSC](#) is an independent non-profit organization dedicated to reducing the number of deaths and injuries in transport in Europe. It provides an impartial source of expert advice on transport safety matters to the EC, the EU parliament, and national

<sup>18</sup> SENSORIS, "Vision," *SENSORIS*, last accessed January 2025, <https://sensoris.org/vision/>

<sup>19</sup> Euro NCAP, "About Euro NCAP," *Euro NCAP*, last accessed January 2025,

<https://www.euroncap.com/en/about-euro-ncap/>



governing. The core activities of ETSC are policy advocacy, research and data collection, safety programs, and public awareness campaigns<sup>20</sup>.

**Relation with M4.2.7:** Although we consider this organization relevant to mention in this report, no direct relationship with the report was established.

**Name: CCAM:** Cooperative, Connected and Automated Mobility

**General Information:** CCAM is a partnership that aims to assess impacts and understand the user and societal effects to harmonize European R&I efforts to accelerate awareness and implementation of innovative CCAM technologies and services, exploiting the full systemic benefits of new mobility solutions enabled by CCAM: increased safety, reduced environmental impacts and inclusiveness<sup>21</sup>.

The [Podium Project](#) aims to accelerate the implementation of advanced CCAM solutions by identifying and assessing the connectivity and cooperation enablers to reach higher levels of automation, advancing PDI technologies, through a multi-connectivity approach<sup>22</sup>.

**Relation with M4.2.7:** The CCAM partnership and Podium Project rely on the provision of accurate, real-time information. As the TN-ITS data chain is directly involved in improving the data aspects that make up this information, any future implementation of CCAM technologies will heavily rely on information provided via this milestone. Another aspect is that for the correct functioning of CCAM systems, a quality base layer is needed. Hence, providing static data via TN-ITS has a direct, undeniable benefit for autonomous and connected systems, giving them additional and, most importantly, precise quality map data.

Another way to connect TN-ITS and CCAM is through HD maps, which enable precise geospatial data exchange. TN-ITS ensures reliable road updates, while CCAM leverages HD maps for accurate positioning and automation. Their integration allows real-time updates from road authorities, enhancing safety and efficiency in ITS. By combining TN-ITS static data with HD maps, CCAM systems gain a continuously updated and high-quality foundation, essential for accurate lane positioning, route planning, and overall operational reliability in automated mobility.

**Name: C-ROADS Platform**

**General Information:** The [C-ROADS Platform](#) allows authorities and road operators to harmonize the deployment activities of cooperative intelligent transport systems (C-ITS) across Europe. Its goal is to achieve the deployment of interoperable cross-border C-ITS services for road users to increase safety on roads and secure the health of people by reducing traffic accidents and increasing traffic flows. The C-ITS systems provide drivers with useful information about their surroundings and traffic situation. The quality, timeliness, and correctness of the information play a crucial role<sup>23</sup>.

<sup>20</sup> European Transport Safety Council (ETSC), "About Us," *ETSC*, last accessed January 2025, <https://etsc.eu/about-us/>

<sup>21</sup> European Commission, *Rolling Plan for ICT Standardisation*, 2024, <https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/intelligent-transport-systems-cooperative-connected-and-automated-mobility-its-ccam-and-2>

<sup>22</sup> Podium Project, "About," Podium Project, last accessed January 2025, <https://podium-project.eu/about/>

<sup>23</sup> C-Roads Platform. "About.", *C-Roads Platform*, last accessed January 2025, <https://www.c-roads.eu/platform/about/about.html>



**Relation with M4.2.7:** TN-ITS supports the C-ROADS Platform’s goals of interoperability, improved road safety, and traffic flows through the standardisation and harmonisation of the data circulated through the TN-ITS data chain. With the C-ROADS Platform publishing its “[C-ITS Services Roadmap for Road Networks in Europe](#)” in April 2024, its future activities will be closely interlinked with this milestone’s information.

**Name: NordicWay**

**General Information:** The project unites public-private partners from the Nordic countries Norway, Sweden, Finland, and Denmark to focus on the common problems they challenge in a unique way suitable for them. The objectives are to jointly deploy C-ITS services and CCAM services in a harmonized way and test them in proof-of-concept pilots <sup>24</sup>.

**Relation with M4.2.7:** Like the Podium Project, the TN-ITS data chain is directly involved in improving the data aspects that make up this information, any future implementation of CCAM services will heavily rely on information provided via this milestone.

**Name: SOCRATES 2.0**

**General Information:** [SOCRATES 2.0](#) (System Of Coordinated Roadside and Automotive Services for Traffic Efficiency and Safety) was a CEF project that was run from 2017 until the end of 2021 that focused on designing and deploying new and extended traffic management measures and mobile/in-car services for road users that aimed to improve traffic, promoting cleaner efficient and safe flows.<sup>25</sup>

**Relation with M4.2.7:** This project helped to provide lessons learned and recommendations for building trust with stakeholders and how to adjust goals for each different Member State where different conditions might apply. Furthermore, in a recent (as of the time of writing this document) workshop, the SOCRATES 2.0 team emphasized the work being done by NAPCORE, further supporting the importance of increasing data availability and quality as a key aspect, and the importance of aligning to the implementation of the RTTI DR and ITS Directive. Finally, the SOCRATES 2.0 team gave some insights on the future challenges that can be faced, such as advanced services, addressing that adequate governance and attractive business models, enabled by procurement policies that focus on EU-wide alignment would help address these challenges.

### 2.2.3.1. METR (updates)

**General Information:** The Management of Electronic Traffic Regulations (METR) is a standard currently under development with the involvement of EU members and the US Department of Transport. METR aims to provide surface transport facility users with a machine-interpretable translation of regional traffic regulations in a global, trustworthy, and authoritative ecosystem.

The scope of METR includes both relatively static rules (e.g., static speed limits) as well as those that are dynamic (e.g., variable speed limits, lane closures at incident scenes). Where

<sup>24</sup> NordicWay, “Home”, *NordicWay*, last accessed January 2025, <https://www.nordicway.net/>

<sup>25</sup> Connected Automated Driving, *European project ‘SOCRATES 2.0’ launched pilot site with improved navigation service*, January 2020, <https://www.connectedautomateddriving.eu/blog/european-project-socrates-2-0-launched-pilot-site-with-improved-navigation-service/>



appropriate, METR is expected to incorporate existing standards (e.g., ISO/TS 19091 for signalized intersections)<sup>26</sup>.

**Relation with M4.2.7:** The METR standard and TN-ITS data chain are closely related in their efforts to improve the management and interoperability of traffic regulations. METR's focus on providing a machine-interpretable format (with particular focus on following the TN-ITS/DATEX II formats) for both static and dynamic traffic regulations, complements TN-ITS's role in standardizing and exchanging road network data. By ensuring that traffic regulations are consistently represented and integrated into ITS applications, METR enhances the overall effectiveness of traffic management systems supported by TN-ITS.

### 2.2.3.2. TISA - RTTI 5-Star Quality Rating

**General Information:** The Traveller Information Services Association (TISA), a globally oriented market-driven membership association, operates as a non-profit entity dedicated to the proactive advancement of traffic and travel information services and products, all while adhering to established standards.

During the Workshop on the Implementation of EU RTTI 2022/670 in April 2023, held in Berlin, TISA assumed responsibility for addressing the critical topic of "How Data Quality Will Improve Usability of Public RTTI Data."<sup>27</sup>

Drawing inspiration from EuroNCAP's 5-Star Vehicle Safety Rating, TISA aims to introduce a 5-star quality rating system with the following objectives:

- a) Empowering Road Authorities and Operators: Provide the road authorities and operators with a practical, user-friendly definition set to assist them in understanding and assessing the quality of their static and dynamic data.
- b) Meeting ITS Service Providers' Requirements: Establish a baseline understanding of the minimum quality standards required by ITS Service Providers for utilizing traffic data effectively.

This approach encompasses the content of RTTI Data Usability, including NAP Functionality, Static Data, and Dynamic Data, along with use-case-specific frameworks (e.g., speed limits, road works, and road closures).

The criteria defined in this framework, including the static data speed limit, can be reviewed through the [RTTI 5 Star Rating Scheme Static Speed Limit table](#) created by TISA.

Some problems and use case issues were detected in this framework and can be reviewed in the material produced during the TISA March 2024 Workshop<sup>28</sup> where the Static Speed Limit accuracy requirements were expanded upon as a use case.

**Relation with M4.2.7:** This milestone can benefit from the quality rating system proposed by TISA; by incorporating similar quality standards for the data, it provides through the TN-ITS data chain, adhering to the requirements set by the RTTI Delegated Regulation (2022/670).

<sup>26</sup> ISO TC 204, *METR Vision*, July 2021, [https://iso-tc204.github.io/iso24315p1/METR\\_Vision.pdf](https://iso-tc204.github.io/iso24315p1/METR_Vision.pdf)

<sup>27</sup> TISA, *RTTI Data Quality Workshop Presentation Slides*, November 2023, [https://tisa.org/wp-content/uploads/TISA-RTTI-Data-Quality-Workshop\\_ALL-SLIDES.pdf](https://tisa.org/wp-content/uploads/TISA-RTTI-Data-Quality-Workshop_ALL-SLIDES.pdf)

<sup>28</sup> TISA, *RTTI Data Quality Workshop Brussels Draft Proposal Slides*, March 2024, [https://tisa.org/wp-content/uploads/TISA-RTTI-Data-Quality-Workshop\\_Brussels\\_slides\\_draft\\_proposal.pdf](https://tisa.org/wp-content/uploads/TISA-RTTI-Data-Quality-Workshop_Brussels_slides_draft_proposal.pdf)



### 2.2.3.3. TISA Guideline ‘Digital Map Quality Assessment Framework for In-Vehicle ISA Systems’

**General Information:** A recent publication from TISA from late November 2024<sup>29</sup> called the “Digital Map Quality Assessment Framework for In-Vehicle Intelligent Speed Assistance (ISA) Systems” serves as a comprehensive guideline developed by TISA to address the critical role of digital maps in supporting ISA technology.

This publication states that as Intelligent Speed Assistance becomes a mandatory feature in vehicles across several regions, including the EU, the accuracy and reliability of digital maps are essential for ensuring compliance, safety, and effective performance. The document explores the complexities of digital map creation, delivery, and assessment, offering a structured approach for stakeholders, such as map providers, regulators, and automotive manufacturers to evaluate map quality in alignment with regulatory requirements and technological advancements.

**Relation with M4.2.7:** M4.2.7 supports the ISA regulation by enhancing the quality and reliability of digital map data through the TN-ITS data chain. The milestone provides tools and methodologies for evaluating data accuracy, completeness, and timeliness, which are critical for ISA compliance. By aligning with standards such as the TISA Digital Map Quality Assessment Framework (which will be discussed later in this milestone), M4.2.7 can potentially contribute to ensuring that spatial and traffic regulation data for ISA systems remain up to date and compliant with regulatory requirements. In particular, in cases of discrepancies between digital maps and the camera system, the feedback loop approach can enable continuous improvements in data quality, directly supporting the successful deployment of ISA systems across Member States.

### 2.2.3.4. TM2.0 (updates)

**General Information: Traffic Management 2.0 (TM2.0)** is an initiative launched in 2014 that aims to improve the reliability of traffic management systems. It focuses on enhancing the quality and accuracy of traffic information, promoting data integrity and security, and enabling efficient information sharing among stakeholders<sup>30</sup>.

In October 2023, TM2.0 organized an online workshop on “Traffic Circulation Plans & Traffic Management Measures & Feedback Loop – Best Practice from the Dutch Projects”.

The workshop outlined [how TCPs as well as TMMs<sup>31</sup>](#) are being digitalised in the Netherlands and what [best practices are resulting from these projects](#). It also discussed the work of Dutch projects that have the feedback loop in interactive Traffic Management and how it works in practice, as their main focus<sup>32</sup>.

**Relation with M4.2.7:** TM2.0 focuses on improving the reliability of traffic management systems. With this milestone providing tools and recommendations for improving the data

<sup>29</sup> TISA, *Digital Map Quality Assessment Framework for In-Vehicle Intelligent Speed Assistance (ISA) Systems*, November 2024.

<sup>30</sup> TM2.0, *TM2.0*, last accessed January 2025, <https://tm20.org/>

<sup>31</sup> TM2.0, *TMC-TCC Workshop TF Perspective*, October 2023, <https://tm20.org/wp-content/uploads/2023/10/TMC-TCC-workshop-TF-perspective-FP.pdf>

<sup>32</sup> TM2.0, *TM2.0 NDW Presentation*, October 2023, [https://tm20.org/wp-content/uploads/2023/10/TM20-workshop-NDW-Presentation\\_without-movie.pdf](https://tm20.org/wp-content/uploads/2023/10/TM20-workshop-NDW-Presentation_without-movie.pdf)



integrity, information, quality, sovereignty, and security of the traffic information being circulated through the TN-ITS data chain as well as the fact that both TM2.0 and this milestone are working on a feedback loop model, the TM2.0 initiative is directly related to M4.2.7 and should be closely monitored for any potential updates that might benefit this milestone and vice versa.

### 2.2.3.5. POLIS RTTI Task Force

**General Information:** POLIS, CROW, and local road authorities across Europe, are working together in this task force, focused on the RTTI Delegated Regulation to analyse and address the challenges raised by the implementation of Real-Time Traffic Information services, and provide their suggestions about how to mitigate them.

In November 2024, they released a new [position paper](#)<sup>33</sup> addressing the role of digital TCPs in ensuring that communication between stakeholders like road authorities and service providers is standardised.

**Relation with M4.2.7:** Like with TM2.0 in the previous section, the digitisation of TCPs plays a crucial role in the management of traffic flow, providing real-time updates on traffic conditions, while also improving the safety and efficiency of traffic flow, by allowing relevant road authorities, service providers, and as a result, end users, to navigate the daily traffic better. This milestone provides recommendations for the improvement of the data quality, integrity, trust, security, and sovereignty criteria, through its feedback loop suggestions and tools analysed related to the TN-ITS data chain. Collaborating with and monitoring other initiatives like the RTTI Task Force allows both groups to benefit from each other.

### 2.2.4. Relevant NAPCORE activities (updates)

Data trust, quality, integrity, security, and sovereignty are mentioned and explored in other NAPCORE activities as well. Therefore, it is important to acknowledge any tasks and deliverables to achieve a harmonized approach to the enhanced data chain of TN-ITS. In the following table a list of the identified quality tasks:

WGs	Task	Outcome / Subtask
WG2	<b>Task 2.2:</b> Definition of requirements concerning data standards, reference profiles, metadata, and support tools	<p>A list of requirements concerning (the use of) data standards, open data, reference profiles, and metadata, developed on a regular annual basis, to be handed over to Sub-WGs on digitalization and/or digitalization organisations, taking data quality into account.</p> <p>The produced report investigates crucial interoperability aspects of the mobility domain, namely data standards, recommended profiles, and</p>

<sup>33</sup> POLIS, *Digitising Traffic Circulation Plans: The Road Ahead*, November 2024, <https://www.polisnetwork.eu/wp-content/uploads/2024/11/RTTI-Report.pdf>



		<p>metadata. Through comprehensive analysis of existing efforts, it identifies gaps in these areas and explores strategies to address them. The document also provides quantitative information regarding the use of standards and profiles, as well as compliance with metadata-related requirements. Drawing from targeted research and expert review, the report offers recommendations to enhance interoperability and streamline mobility data exchange, particularly those listed in the ITS directive delegated regulations.</p> <p>The M2.7 report was finalized and ready for review and NAPCORE approval (September 2024).</p>
	<p><b>Task 2.3: NAP Architecture</b></p>	<p>A set of functional and technical requirements to harmonise the functions and interfaces of NAPs.</p> <p>Milestone 2.9, titled "Harmonisation of EU NAP architectures and first layout of potential NAP federation," outlines the harmonisation activities, technical procedures, and developmental steps taken to achieve a NAP reference architecture. This NRA consolidates all NAPCORE National Access Point harmonisation activities.</p> <p>The milestone report (M2.9) was finalized and approved by the SCOM in May 2024.</p>
<p><b>WG3</b></p>	<p><b>Task 3.2: European NAPs data quality</b></p>	<p>Subtask 3.2.1 – Quality Framework where quality criteria and levels of service of the EU-EIP were considered. This includes the establishment of generic Quality Frameworks for various ITS domains, containing agreements and definitions for quality criteria and (minimum) requirements (i.e., covering aspects such as geographic coverage, timeliness, latency, position accuracy, and error level). These frameworks build upon the outcomes of the EU EIP platform in this topic (i.e., Quality Frameworks for all ITS Directive’s priority services and C-ITS services) considering that these outcomes may need further validation and maturity. Besides, further frameworks are newly established, e.g., for emerging data categories such as UVAR. Starting from reviewing current achievements in the data quality field and identifying existing gaps, some preparatory works are done first, setting the scope of the Quality Frameworks to be established, and including the identification and analysis of the relevant needs of all actors involved in the ITS value chain (including but</p>

		<p>not limited to e.g., public and private data providers or relevant associations).</p> <p>The final deliverable (M3.8) from this work item will be a set of Quality Frameworks for different data domains and use cases, provided as an online repository.</p> <hr/> <p>Subtask 3.2.2 – Guidance &amp; best practices for quality assessment. Efficient ways to assess individual NAP datasets have not been explored on a wide basis, i.e., there is a lack of experience and common understanding of how to apply the Quality Frameworks in practice, e.g., by NAP operators or by the National Bodies. This subtask will involve best-practice research and practitioners’ exchange, to provide guidelines on how to introduce, monitor and enforce Quality Assessment, regarding NAP datasets at individual organisations, accounting also for differences in the application of related standards. The guidelines will be accompanied by pilot assessments of selected, real-life NAP data sets, to prove and demonstrate the identified Quality Assessment methods. The outcomes from such assessment will be also used as a feedback loop to the above-mentioned Quality Frameworks, i.e., the Frameworks will be validated and eventually updated upon the assessment results.</p> <p>The final deliverable (M3.9) from this work item will be a report called “Quality Framework Application Guideline”.</p> <hr/> <p>Subtask 3.2.3 – Quality certification for NAP datasets                  This task will concretise and formalise the above-mentioned Quality Assessment methods, as a model for a neutral and harmonised Quality Certification process. Hence, it will provide a guideline about Quality certifications The milestone (M3.10) Report on pilot data quality certifications will be available by the end of NAPCORE.</p>
	<p><b>Task 3.3:</b> Data access and reuse</p>	<p>This task will investigate commonly accepted frameworks and technical options to achieve fair, trusted, and enhanced accessibility to ITS-related data through European NAPs and will create added-value visualization tools to be used by NAP operators, data providers, and data consumers. The milestone</p>

		(M3.11) M3.11 Terms and conditions for data reuse will be available by the end of NAPCORE.
<b>SWG4.1</b>	<b>Task 4.1.5:</b> Modelling and Usability	These tasks will assess at least the following topics for modifications of the D2 methodology for the following developments extending and improving the usability of the DATEX II encoded data: - Trust and data authenticity / Security.
	<b>Task 4.1.6:</b> Encoding & Transfer	
<b>SWG4.4</b>	<b>Task 4.4.2.4:</b> Draft Specification	Work Item Accompanying Guideline regarding metadata quality criteria.
<b>WG5</b>	<b>Task 5.3:</b> Quality and evaluation criteria	<p>Task 5.3 “Define (common) quality and evaluation criteria for Compliance Assessment” is completed, the results are presented in the Milestone Report M5.4 “Common quality &amp; evaluation criteria for compliance assessment defined”, which was approved by the Steering Committee in September 2023.</p> <p>The main goal of the report was to define common quality and evaluation criteria for Compliance Assessment. The Delegated Regulations (EU) of the ITS Directive, state that the quality of data is very important, but they do not provide guidance on how quality is defined in this context. Working Group 5 reviewed and analysed the quality requirements of the Delegated Regulations as well as practices and approaches National Bodies currently have toward those requirements. As a result, 15 quality parameters have been defined and included in the Compliance Assessment forms. They provide the framework for assessing quality within the assessment of compliance with the Delegated Regulations and should be taken as a reference by the National Bodies.</p>

Table 1 - Quality and Trust Tasks from the NAPCORE Project

### 2.2.5. Mobility Data Space (updates)

The Mobility Data Space (MDS)<sup>34</sup> is a crucial initiative within the European Union, designed to enhance data interoperability and sharing in the transport sector. It aligns with the European Data Strategy and the Sustainable and Smart Mobility Strategy, aiming to create an integrated digital infrastructure that supports efficient, sustainable, and resilient mobility across Europe.

<sup>34</sup> Mobility Data Space. "Mobility Data Space." *Mobility Data Space*, last accessed January 2025  
<https://mobility-dataspaces.eu/mobility-data-space>



The MDS can be seen as an evolving ecosystem where data flows between stakeholders, each contributing to and benefiting from the increased value of shared data.

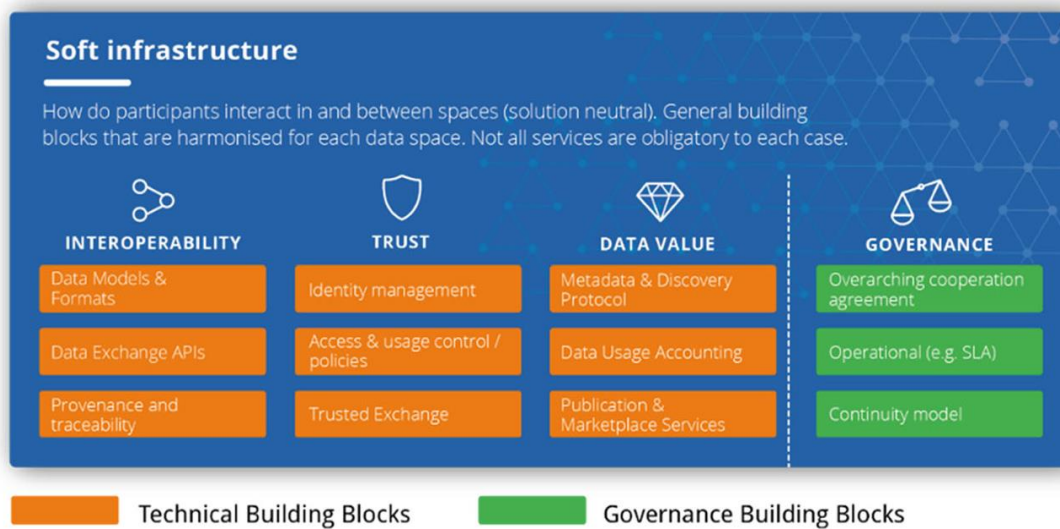


Figure 2 - Building blocks for data spaces (©2021, International Data Spaces Association)

TN-ITS plays a fundamental role within the MDS by facilitating the regular updating and exchange of transport network spatial data. This data is crucial for various applications, including traffic management, map updates, and the development of connected and autonomous vehicles. Within the MDS framework, TN-ITS can be seen as an essential component that ensures the continuous and accurate flow of spatial data, making it indispensable to the entire ecosystem.

### Integration of TN-ITS into the European Mobility Data Space (EMDS)

TN-ITS is a key element of the [deployEMDS](https://deployemds.eu)<sup>35</sup> project, co-funded by the EU Digital Europe Programme. This project focuses on creating an operational data space with robust infrastructure, governance, and processing mechanisms. The role of TN-ITS in this structure is to provide high-quality, reliable spatial data, supporting the EU's digital sovereignty.

The Innovation and Scaling Group (ISG), operating under the deployEMDS initiative, plays a crucial role in promoting innovation and expanding the implementation of TN-ITS across the European Mobility Data Space. By focusing on capacity building, standardization, and stakeholder engagement, the ISG helps to ensure that TN-ITS can be effectively integrated and scaled within the EMDS.

The real-world implementation of TN-ITS is underway in several pilot cities and regions, including Barcelona, Milan, and Lisbon. In these regions, TN-ITS data supports improvements in urban mobility, traffic management, and the accuracy of digital maps. These pilots are essential for demonstrating the practical benefits of TN-ITS within the EMDS framework and showcasing its potential for broader application.

### The Role of EDIC in Expanding TN-ITS within the MDS

<sup>35</sup> DeployEMDS, "Project," *DeployEMDS*, last accessed January 2025, <https://deployemds.eu/project/>



This project has received funding from the European Commission's Directorate General for Transport and Mobility under Grant Agreement no. MOVE/B4/SUB/2020-123/SI2.85223

The [European Digital Infrastructure Consortium \(EDIC\)](#)<sup>36</sup> is a proposed project aimed at establishing a unified framework for the expansion and implementation of initiatives like TN-ITS across the EU. Though not yet fully established, EDIC, or a similar project, could provide significant benefits for stakeholders within the Mobility Data Space (MDS), including:

- **Cost Efficiency:** By centralizing resources and expertise, EDIC could lower overall costs related to data exchange and infrastructure development.
- **Alignment and Standardization:** EDIC would promote alignment in database attributes, tools, and processes, ensuring consistency and interoperability across the MDS.
- **Political Stability:** With commitments from Member States, EDIC would offer a stable and politically supported framework, essential for long-term success.
- **Focused Expertise:** A dedicated consortium like EDIC would ensure a concentrated focus on developing and deploying high-quality data tools and processes.
- **Representation and Advocacy:** EDIC could act as a representative body to negotiate with service providers, ensuring data quality and compliance with European laws.
- **European Engagement:** EDIC would enhance European collaboration and commitment to digital infrastructure, aligning initiatives like TN-ITS with broader EU strategies.

While EDIC is still a proposal, its potential to facilitate strategic collaborations between public authorities, private entities, and end-users should not be underestimated. These partnerships would be crucial for the continued development and integration of TN-ITS, ensuring that it evolves to meet the changing needs of the MDS.

#### 2.2.5.1. Benefits of TN-ITS in the MDS

- **Data Interoperability and Standards** - One of the primary benefits of TN-ITS within the MDS is its ability to facilitate interoperability across different data systems. TN-ITS adheres to common standards, enabling seamless data exchange between various stakeholders, and ensuring that transport network data is effectively utilized across the EU in a trustworthy manner. This benefit will be even more prominent with the alignment plan between TN-ITS and DATEX II standards.
- **Data Quality and Reliability** TN-ITS enhances the quality and reliability of data within the MDS by providing timely and accurate updates to transport network data. This ensures that the information used in applications such as navigation systems and traffic management is both reliable and up-to-date.
- **Data Security and Sovereignty** Data security and sovereignty are critical concerns in the MDS. TN-ITS addresses these concerns by ensuring that data is managed and shared in a secure environment, compliant with EU governance and data protection regulations. This not only protects the integrity of the data but also ensures that it remains under the control of relevant authorities.

<sup>36</sup> European Commission. "European Digital Innovation Centres (EDIC)." *Digital Strategy*, December 2024, <https://digital-strategy.ec.europa.eu/en/policies/edic>



### 2.2.5.2. TN-ITS Use Cases

- **Digital Map Updates:** TN-ITS plays a critical role in keeping digital maps accurate and up to date. By providing consistent and reliable data updates, TN-ITS supports essential applications such as navigation systems, traffic management, and other services that rely on precise spatial data.
- **Integration with Connected and Autonomous Vehicles:** The data provided by TN-ITS is vital for the safe and efficient operation of connected and autonomous vehicles. These vehicles require accurate, real-time data to navigate complex environments, making TN-ITS a key enabler of future mobility solutions.
- **Urban Planning Support:** TN-ITS data is instrumental in informing urban planning decisions and helping to develop sustainable and efficient transportation systems. By providing detailed spatial data, TN-ITS supports planners in optimizing infrastructure and improving overall mobility in urban areas.
- **The Role of Data Connectors:** Data connectors play a crucial role within the Mobility Data Space (MDS) by facilitating sovereign data exchange between different participants in the ecosystem. The Data Space Connector (DSC) is an example of open-source software that enables this data exchange with continuous control by the data provider. Even after the data has been shared, the provider retains control over what happens to their data, ensuring data security and sovereignty. Connectors, therefore, are essential components in ensuring that TN-ITS can operate within a dynamic and secure data ecosystem.

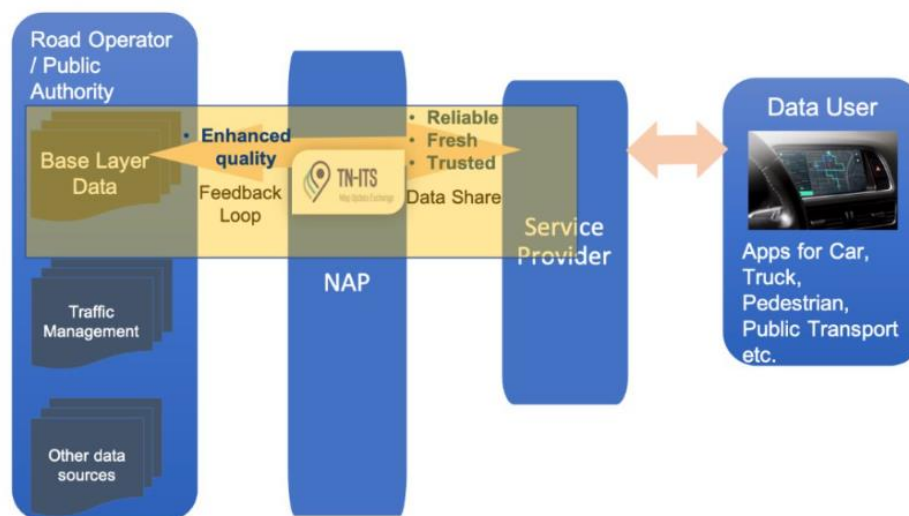


Figure 3 - Dataspace Connector (DSC)

- **Road operator / Public authorities:** Authorities, such as governmental bodies or regulatory agencies, act as both data providers and consumers. The (out)connector enables authorities to share data, such as road infrastructure updates or traffic regulations, with service providers or other entities within the MDS. The (in)connector allows them to receive data and support functions such as traffic management or infrastructure planning.
- **National Access Points:** NAPs serve as critical nodes within the MDS, acting as intermediaries that facilitate data exchange between national-level data sources and

broader European systems. The (out)connector at a NAP enables the dissemination of national datasets, in TN-ITS format for example, to other EU Member States or service providers, while the (in)connector allows NAPs to receive and integrate data from other countries or central EU databases.

- **Service Providers:** Service providers, such as navigation system developers or autonomous vehicle operators, rely on data from multiple sources within the MDS. The (out)connector allows these providers to share processed data or services with other stakeholders, while the (in)connector enables them to gather raw data from authorities, NAPs, and other sources.
- **End Users:** End users, including drivers, pedestrians, and public transport operators, access the data through applications provided by service providers. These users rely on the reliable, fresh, and trusted data facilitated by the TN-ITS system to make informed decisions. Their interaction with the data completes the feedback loop, providing critical input that can help improve data quality and relevance.

The MDS framework supports these interactions by ensuring that the data exchanged via these connectors is interoperable, secure, and aligned with EU data governance standards. MDS functionality, therefore, includes not just the technical infrastructure to facilitate data exchange but also the policies, standards, and legal frameworks that ensure data sovereignty and trust across all interactions. This functionality underpins the entire ecosystem, making it possible for TN-ITS to operate effectively within the broader Mobility Data Space.

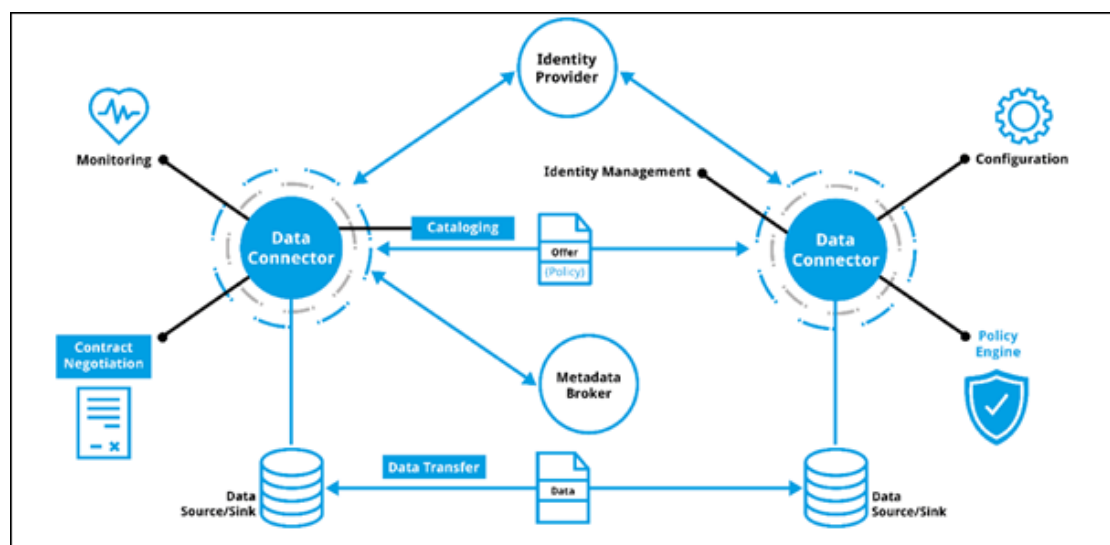


Figure 4 - An example diagram of data connectors in MDS<sup>37</sup>

### External Standards and Data Quality

TN-ITS format integrates with various external standards, such as SENSORIS, ADASIS<sup>38</sup>, and TISA, to ensure that data quality is maintained across the ecosystem. The adoption of these

<sup>37</sup> Otto et al, *Designing data spaces*, Springer September 2021, pp 352

<https://link.springer.com/content/pdf/10.1007/978-3-030-93975-5.pdf?pdf=button>

<sup>38</sup> ADASIS, *Organisation*, last accessed January 2025, <https://adasis.org/organisation/>



standards within the MDS helps maintain a high level of data integrity and supports the automation and improvement of data ratings.

### 2.2.5.3. Challenges and Future Opportunities

Integrating TN-ITS into the Mobility Data Space (MDS) presents several challenges, including technological and regulatory barriers. Addressing these challenges requires ongoing innovation, collaboration, and a strategic approach to standardization and cross-border data sharing.

#### **Technological and Regulatory Barriers:**

One of the primary challenges is the need to harmonize data formats and standards across different regions and stakeholders. The diversity in data formats and the lack of a unified approach complicate the process of ensuring consistent and high-quality data exchange. Additionally, the current digital infrastructure in many regions is inadequate to handle the scale and complexity of data required by modern mobility systems.

#### **Stakeholder Engagement:**

Engaging diverse stakeholders, such as Member States, Service Providers, Map Makers, and Road Authorities, is a critical challenge for the successful deployment of TN-ITS within the MDS. Each stakeholder group has different priorities, resources, and levels of expertise, which can create obstacles in aligning their efforts toward a common goal. For instance, some stakeholders may be more focused on traditional solutions, while others may lack the capacity or incentives to adopt new data-driven approaches.

#### **Importance of Governance and Collaboration:**

Proposals like the European Digital Infrastructure Consortium (EDIC) and the [Innovation and Scaling Group \(ISG\)](#)<sup>39</sup> are crucial in overcoming these challenges with strategic partnerships. EDIC, as previously discussed, offers a framework for centralized resource management, standardization, and political stability across Member States. By providing a unified approach to data exchange and infrastructure development, EDIC can help reduce costs and ensure the consistent application of standards throughout the EU.

The ISG, which operates under the deployEMDS initiative, further supports these goals by fostering innovation and scaling successful pilot projects. The ISG emphasizes the need for mindset shifts, capacity building, and the adoption of common data standards. It also addresses critical issues such as data monetization, legal and security concerns, and the development of robust data quality assurance frameworks. The ISG's efforts in engaging stakeholders, promoting standardization, and enhancing data infrastructure are essential for the successful integration of TN-ITS within the MDS.

#### **Opportunities for Integration with Emerging Technologies:**

There are significant opportunities for TN-ITS to expand into new areas by integrating with emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT). These

---

<sup>39</sup>DeployEMDS, *Innovation and Scaling Group launch by deployEMDS*, April 2024,

<https://deployemds.eu/innovation-and-scaling-group-launch-by-deployemds/>



This project has received funding from the European Commission's Directorate General for Transport and Mobility under Grant Agreement no. MOVE/B4/SUB/2020-123/SI2.85223

innovations could further enhance the capabilities of TN-ITS and its contribution to the MDS, opening new avenues for data-driven mobility solutions.

TN-ITS plays a crucial role in the European Mobility Data Space, driving forward the EU's digital and mobility strategies. By enhancing data interoperability, quality, and security, TN-ITS ensures that the MDS can effectively support the future of European transport.

### 3. TN-ITS Data Chain

In this chapter, the evolution of the TN-ITS Data Chain is explored by introducing new roles with updated names and descriptions which are now aligned with the RTTI Delegated Regulation. We provide comprehensive definitions of the Data Chain stages from the TN-ITS perspective and an enhanced diagram that illustrates the TN-ITS Data Chain, encompassing roles, the feedback loop, and the critical data aspects.

Furthermore, we conduct an in-depth assessment of potential scenarios involving the feedback loop within the TN-ITS Data Chain, supported by detailed diagrams for each scenario. This analysis aims to elucidate how feedback mechanisms contribute to the continuous improvement and efficiency of the TN-ITS data exchange mechanism.

#### 3.1. TN-ITS Stakeholders and Their Harmonized Roles

One of the primary goals of the NAPCORE project is to enhance the interoperability of mobility data in Europe with mobility data standard harmonization and alignment. Also, NAPCORE aims at increasing access to and expanding the availability of mobility related data by coordinated data access and better harmonization of the European NAPs. Therefore, Task Group 4.2.4 decided to adopt the existing roles in the RTTI Delegated Regulation, adapted to the TN-ITS Data Chain, so that this alignment and harmonization become a reality.

All studies and analyses in this Milestone will be based on these RTTI compliant new TN-ITS roles. Next, the new roles will be presented along with their definitions, as well as the old roles replaced from M4.2.6 (based on the TN-ITS Go project). For definitions of the old roles, please refer to the previous Milestone 4.2.6.

New Role	RTTI / TN-ITS Description	Replaced Role (M4.2.6)
<b>Data Holders</b>	The data holder means any legal person, data subject, or public or private entity who has the right to grant access to or to share the data related to infrastructure, regulations, and restrictions listed in the RTTI Delegated Regulation Annex under its control, under applicable Union or national law.	Data Owners
<b>Data Users</b>	The data user means any road authority, road operator, tolling operator, service provider, and digital map producer, or any other entity using data to create real-time traffic information or, where allowed by the terms and conditions determined by the data holder, using the data for other mobility related purposes.	Data Providers
<b>Access Point (set up by a Member State)</b>	An access point means a digital interface where data listed in the RTTI Delegated Regulation Annex, together with the corresponding metadata, are made accessible for re-use to data users, or where the sources and metadata of these data are made accessible for re-use to data users. NAP is one such example.	Data Access Enablers

<b>Service Providers</b>	A service provider means any public or private provider of a real-time traffic information service, excluding a mere conveyer of data-to-data users.	Data Consumers
<b>End-Users</b>	The end-users mean any road user, natural or legal person, who has access to real-time traffic information services.	Road End Users

Table 2 - List of New Stakeholder Roles for TN-ITS data chain and description

### 3.1.1. Role-Based Stakeholder Grouping

The data holders and data users share the same list of stakeholders as this was the approach adopted in the previous Milestone, and because the distinction between the two depends on the reality in each Member State. Here is the list of potential stakeholders of the TN-ITS data chain assembled by the new roles.

New Roles	TN-ITS Stakeholders
<b>Data Holders &amp; Data Users</b>	<ul style="list-style-type: none"> <li>- Road Authorities (National, Regional, and Local level)</li> <li>- National Mapping Agencies</li> <li>- OEM (Original Equipment Manufacturer)</li> <li>- Concessionaires (i.e. private road operators)</li> <li>- Other map providers/makers (e.g. Google, Open Street Map, TomTom, etc)</li> <li>- IoT Network</li> <li>- Research Institutions and Universities (utilize data for studies and analyses)</li> <li>- Private Companies (involved in data analysis and traffic data-based solutions development)</li> </ul>
<b>Access Point</b> (set up by a member state)	<ul style="list-style-type: none"> <li>- National Access Points (NAPs) set up by a Member State</li> <li>- Open Data Aggregator Platforms</li> <li>- Private Data Marketplaces</li> </ul>
<b>Service Providers</b>	<ul style="list-style-type: none"> <li>- Other map providers/makers/producers (e.g. Google, Open Street Map, TomTom, etc)</li> <li>- Land Surveying and Cadastral</li> <li>- App Developer (Start-up)</li> <li>- Data Brokers</li> <li>- Open Data initiatives</li> <li>- Regulatory Bodies and Public Authorities (Internal Consuming)</li> <li>- Vehicle Manufacturers and TIER1 Suppliers</li> </ul>
<b>End-Users</b>	<ul style="list-style-type: none"> <li>- Private drivers</li> <li>- Businesses drivers (Logistics and Transportation Companies)</li> <li>- Micro mobility users</li> <li>- Pedestrians and Cyclists</li> </ul>

Table 3 - List of Potential Stakeholders assembled by the new roles

In addition to the stakeholders directly involved in the TN-ITS data chain, other stakeholders may influence its functioning. These stakeholders, while not directly linked to the data chain itself, can still play a crucial role in shaping its outcomes. For example, road safety associations (EuroRAP<sup>40</sup>, ETSC, VIAS<sup>41</sup>), consumer organizations (EuroNCAP), platforms and partnerships (CCAM single platform), and ICT suppliers (MS subcontractors and coding companies), are stakeholders that may have indirect but impactful involvement in the TN-ITS ecosystem. Their actions, policies, and collaboration can contribute to the success and effectiveness of the data chain in achieving its objectives. Therefore, considering the broader stakeholder landscape is essential to comprehensively understand the dynamics and potential implications of the TN-ITS data chain.

### 3.2. Data chain stages

Following the TN-ITS roles approach, the same methodology was applied to the five TN-ITS stages of the data chain. For each stage, a clear definition was established and agreed upon by the task group members. Below, we present the five recognized stages of the data chain along with their consensus definitions.

- **Data Collection:** Involves gathering data manually, from sensors, cameras, connected vehicles, and includes data regarding changes and new entries in road infrastructure and road attributes.
- **Data Processing:** Encompasses the transformation, cleansing, and enrichment of raw data to derive meaningful insights. During this stage, data is processed and converted to suit standardized exchange frameworks such as TN-ITS.
- **Data Exchange:** Involves the secure transmission of processed data among different stakeholders within the TN-ITS ecosystem. The processed data are exchanged using an XML format through a TN-ITS national portal and/or through the MS NAPs.
- **Data Integration:** This is the stage where map providers and other data users process and integrate data into their digital maps, focusing on merging various datasets from multiple sources into a cohesive and consistent format.
- **Data Usage:** Involves the utilization of integrated data in updated digital maps to support various applications and platforms, such as traffic management, navigation systems, and policy planning.

### 3.3. Feedback Loop

In the previous Milestone (4.2.6) of this task 4.2.4, a preliminary analysis of the Feedback Loop within the TN-ITS data chain was conducted. In this Milestone, the goal is to build upon the findings of Milestone 4.2.6 by providing a more comprehensive examination. To extend the analysis and facilitate internal discussion on this task, a Feedback Loop Workshop was conducted. This workshop generated numerous inputs and ideas on the topic, contributing significantly to the depth and breadth of the examination in this Milestone.

---

<sup>40</sup> Road Safety Foundation, *What is EuroRAP*, last accessed January 2025, <https://roadsafetyfoundation.org/eurorap-uk/what-is-eurorap/>

<sup>41</sup> Vias, *About Vias institutet*, last accessed January 2025, <https://www.vias.be/en/about-vias/>



**Note:** What follows is based on the findings of this workshop, however, it is imperative to note that other platforms, such as Google Maps and Waze, or other groups, such as the RTTI Taskforce are also working on their versions of a feedback loop so this should be taken in as suggestions only for TN-ITS data chain rather than a definitive proposal for the broader ITS community.

### 3.3.1. Introduction to the Feedback Loop

The feedback loop serves as a proactive measure to identify, address, and mitigate weaknesses across the data chain. It enhances the quality, reliability, and user satisfaction of its data-driven services. A deeper investigation into the legislative and technical context was carried out to ensure a clear understanding of the regulatory framework governing the TN-ITS data chain. Additionally, various types of feedback loops were identified and described, highlighting their functions and implications. Finally, possible scenarios that could emerge from the interactions between different actors and their roles are presented and analysed, providing a detailed mapping of these relationships and their impact on the TN-ITS data chain. Tools for implementing the feedback loop are suggested but analysed in detail in a subsequent chapter of this Milestone.

### 3.3.2. Legal context

A thorough understanding of the regulatory framework is essential for ensuring compliance and optimizing the effectiveness of the feedback loop. Much of the information obtained for this topic was based on the ITS Directive 2010/40 and the RTTI DR 2022/670. Various suggestions and articles highlight the need for different stakeholders, in specific roles, to collaborate in harmony to address issues through communication channels in TN-ITS data and related services, thereby improving their quality. The legal relationship with the feedback loop is well illustrated in Articles 4 and 5 of the RTTI DR 2022/670<sup>42</sup>, where the TN-ITS format is recommended. It states, "Data users... and data holders shall collaborate to ensure that any inaccuracies related to the data are signalled without delay to the data holder from which the data originates."

Additionally, it is important to consider other relevant legal frameworks, such as the [General Data Protection Regulation \(GDPR\)](#)<sup>43</sup>. For instance, GDPR compliance may protect the users in the process of reporting data inaccuracies, thereby ensuring the accuracy and legal integrity of the data managed within the TN-ITS feedback loop. National transport regulations across different EU member states may also influence how feedback loops are implemented, especially regarding real-time data reporting for public safety.

---

<sup>42</sup> Commission Delegated Regulation (EU) 2022/670, pp 7-8, February 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0670>

<sup>43</sup> Commission Delegated Regulation (EU) 2016/769, April 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504>



### 3.3.3. Types of Feedback Loop

This subchapter categorizes and describes various types of feedback loops, highlighting their functions to understand their roles in improving data chain processes. The feedback loops between stakeholders/roles in the TN-ITS data chain have been grouped into two main categories: syntax feedback loops and semantic feedback loops. This categorization helps in systematically addressing different aspects of data validation and communication.

A **syntax feedback loop** ensures that data exchanged between stakeholders adheres to predefined structural and formatting rules. It checks for correct syntax, such as grammar, punctuation, coding formats, and the presence of required fields, ensuring that the data is syntactically valid and can be processed without errors.

A **semantic feedback loop** ensures that the data exchanged between stakeholders accurately represents the intended information and is meaningful. It checks for the correctness, consistency, and relevance of the data's content, ensuring that the information conveyed aligns with real-world entities and concepts understood by all stakeholders. It gives relevant feedback regarding the usefulness and overall experience of a user with the service.

The table below provides a clear overview of the types of feedback associated with each category.

M4.2.6	Type of Feedback	Description
<b>Syntax Feedback Loop</b>	Data Accuracy Feedback	Reports on incorrect or outdated information in the dataset.
	Data Completeness Feedback	Feedback on missing data or incomplete datasets.
	Data Timeliness Feedback	Reports on outdated data that need updating.
<b>Semantic Feedback Loop</b>	Usability Feedback	Suggestions on how to improve the accessibility and usability of the data.
	Interoperability Feedback	Feedback on issues related to data integration and compatibility with other systems/formats.
	Performance Feedback	Reports on the performance of data platforms.
	Relevance Feedback	Feedback on the relevance and usefulness of the provided data.
	User Experience Feedback	General feedback on the overall experience of using the data services.

Table 4 - Overview of the types of feedback with each category

An additional distinction needs to be made at this stage which is the difference between external feedback and internal feedback. During the expert discussion, it was highlighted that the distinction between a Data User and a Data Holder is blurred, and one entity can assume both roles. Any feedback within these two entities can be treated as *internal feedback* and labelled as such. Whereas feedback shared by the Service Provider is coming from an external

entity. For this work, external feedback is simply labelled as *feedback*. These terms will be used as such in the scenario description.

### 3.3.4. Feedback Loop Possible Scenarios

Potential feedback scenarios that may arise from the interactions between different stakeholders and their roles within the TN-ITS data chain are defined in this section. A detailed mapping of these relationships and their impacts is reported, offering insights into how feedback loops can influence the overall data chain.

#### **Scenario 1: End-User initiates a feedback message**

*Example in a real-world TN-ITS context: Road Closure Data Accuracy - A Road is temporarily closed for maintenance, but this closure is not properly recorded in the TN-ITS system. A syntax feedback loop from an end-user (e.g., a driver) could report this omission directly to the Data Holder or the Service Provider. The data holder quickly updates the system, ensuring that routing services can accurately redirect traffic.*

- **Option I:** End-user Feedback is directly shared with the Data Holder/Data User:
  - ✓ **Method:** This process is facilitated through a special Application Programming Interface (API) (step 1) designed for direct communication between the end user and the data holder/data user.
  - ✓ **Processing the Feedback:** Upon receiving the feedback, the data holder/data user analyses and processes the information (step 2) through internal feedback mechanisms. This step involves assessing the feedback for validity, relevance, and any required actions to address the concerns raised.
  - ✓ **Response to the End-User:** After processing the feedback, the data holder/data user responds to the end-user (step 3). This response includes details about the type of feedback received, the actions taken, and any resolutions or updates. This step completes the feedback loop, ensuring the end user is informed about the outcome.

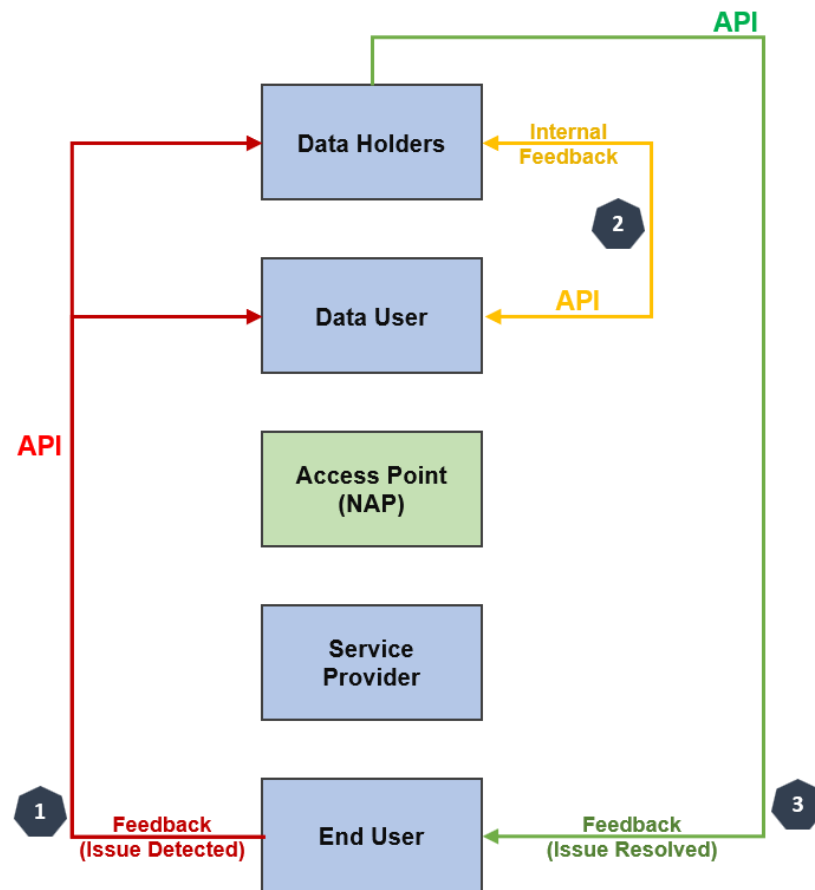


Figure 5 - Feedback Loop Scenario 1 Option I

- **Option II:** End-user feedback is directed towards the Service Provider:
  - ✓ **Method:** In this approach, feedback from the end-user is initially directed to the service provider (step 1) via a Graphical User Interface (GUI) of a mobile application or web interface. This interface allows users to easily submit their feedback.
  - ✓ **Processing the Feedback:** The service provider plays a crucial role in this process by verifying the feedback received from multiple users and collating it into a structured format. This step ensures that the feedback is comprehensive, and any redundant or duplicate feedback is managed efficiently. The service provider then forwards the verified and collated feedback to the data holder/data user (step 2) using the special API designed for such interactions. Upon receiving the feedback, the data holder/data user processes the information similarly to Option 1 (step 3) through internal feedback mechanisms. This involves analysing the feedback and determining the necessary actions.
  - ✓ **Response to the End-User:** After processing the feedback, the data holder/data user response, to the service provider (step 4) can be a simple acknowledgment or include details about the feedback received, the actions planned or taken, and any resolutions or updates. The service provider then communicates this information back to the end user, completing the feedback loop.

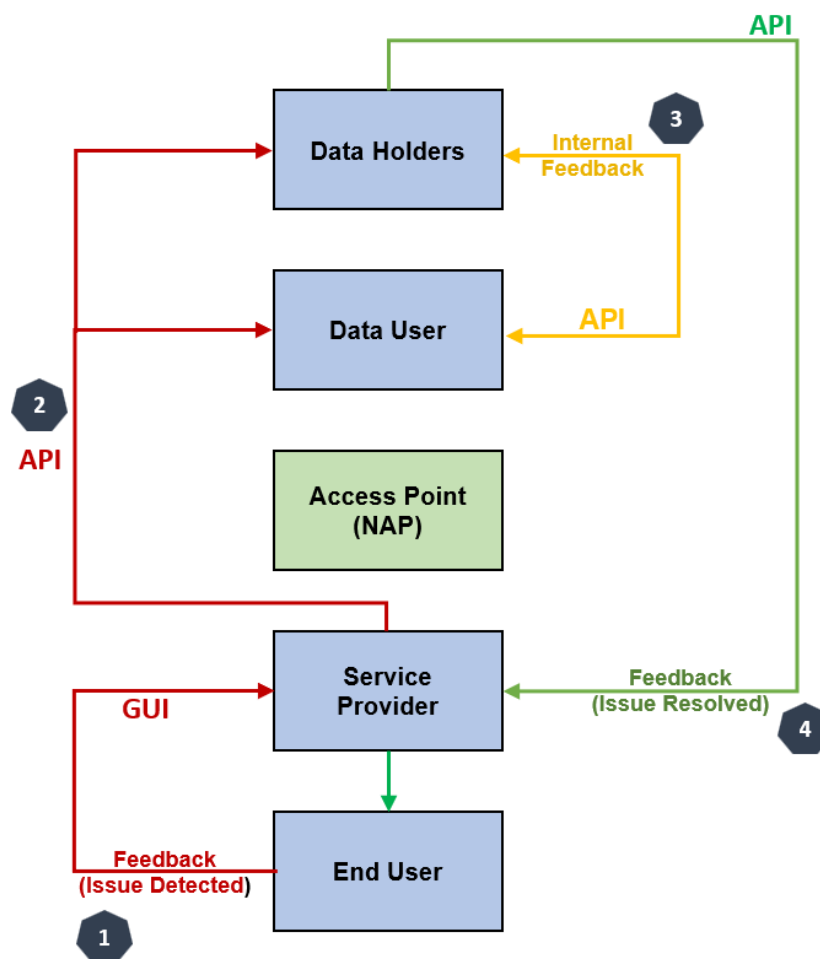


Figure 6 - Feedback Loop Scenario 1 Option II

To align efforts with TISA on this topic, a working document titled, ‘Digital Map Quality Assessment Framework for In-Vehicle Intelligent Speed Assistance (ISA) Systems’ is critically evaluated to identify synergies or potential conflicts.

The report highlights the importance of having a reliable digital map for ISA. It specifies that ISA systems can be configured in three ways: vehicle camera-based, digital map-based, or a fused system. When inputs from the camera and map conflict, most ISA systems prioritize the camera. However, third-party research, including findings from the European Automobile Manufacturers Association (ACEA), indicates that cameras achieve only about 50% accuracy<sup>44</sup> due to various challenges such as obstructions<sup>45</sup>, poor lighting, or difficulty interpreting variable or conditional speed limits. In addition, it is also necessary to consider the possibility of fraudulent traffic signs or a cyber-attack on a Hardware or Software part. In cases where the camera is obstructed or its reading is less reliable, the map-based system can take

<sup>44</sup> Johannes Bauer, *Feedback from: European Automobile Manufacturers Association ACEA*, 2021, [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12222-Vehicle-safety-technical-rules-test-procedures-for-intelligent-speed-assistance/F2256534\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12222-Vehicle-safety-technical-rules-test-procedures-for-intelligent-speed-assistance/F2256534_en)

<sup>45</sup> Demuyne Vinnent, *Why quality of digital maps matters for Intelligent Speed Assistance (ISA) compliance*, 2021 <https://www.tomtom.com/newsroom/product-focus/why-quality-of-digital-maps-matters-for-isa-compliance/>

precedence, provided its data is verified and has a high confidence level. If conflicting speed limit information arises between the camera and the map, and neither source is obstructed or unreliable, one possible suggestion could be to utilise the proposed feedback loop scenario 1 option II. The end-user would provide feedback to the service provider who would then reevaluate the data with the data user and/or data holder to validate the correct speed limit for the specific road segment. The data user and/or data holder can then respond accordingly by either correcting the on-site speed limit signs or updating their database to ensure that the digital maps reflect the correct information and provide their feedback accordingly. Since some Road Operators do not yet have tools to detect potential problems with their traffic infrastructure, even simple feedback informing them about such issues is valuable.

In both options from scenario 1, the feedback loop is designed to ensure effective communication and resolution of issues raised by end users, enhancing the overall quality and reliability of the data and services provided.

### **Scenario 2: Service Provider initiates a Feedback Message**

*Example in a real-world TN-ITS context: Traffic Sign Update – Consider a case in which a traffic sign's speed limit is updated, but this change is not reflected in the national database. A semantic feedback loop initiated by a navigation service provider could alert the data holder about the discrepancy. The data holder then updates the database, and this update is communicated back to the navigation service provider, ensuring all systems reflect the correct information.*

- **Option I: Service Provider feedback is directly shared with the Data Holder/Data User:**
  - ✓ **Method:** The feedback from the service provider is directly shared with the data holder/data user via a special API (step 1) designed for such direct interactions.
  - ✓ **Processing the Feedback:** Upon receiving the feedback, the data holder/data user processes it (step 2), through internal feedback mechanisms, by analysing the information, verifying its accuracy, and determining any necessary actions to address the issues raised.
  - ✓ **Response to the Service Provider:** After processing the feedback, the data holder/data user responds to the service provider (step 3). This response includes details about the type of feedback received, the actions taken, and any resolutions or updates. This step completes the feedback loop, ensuring that the service provider is informed about the outcome.

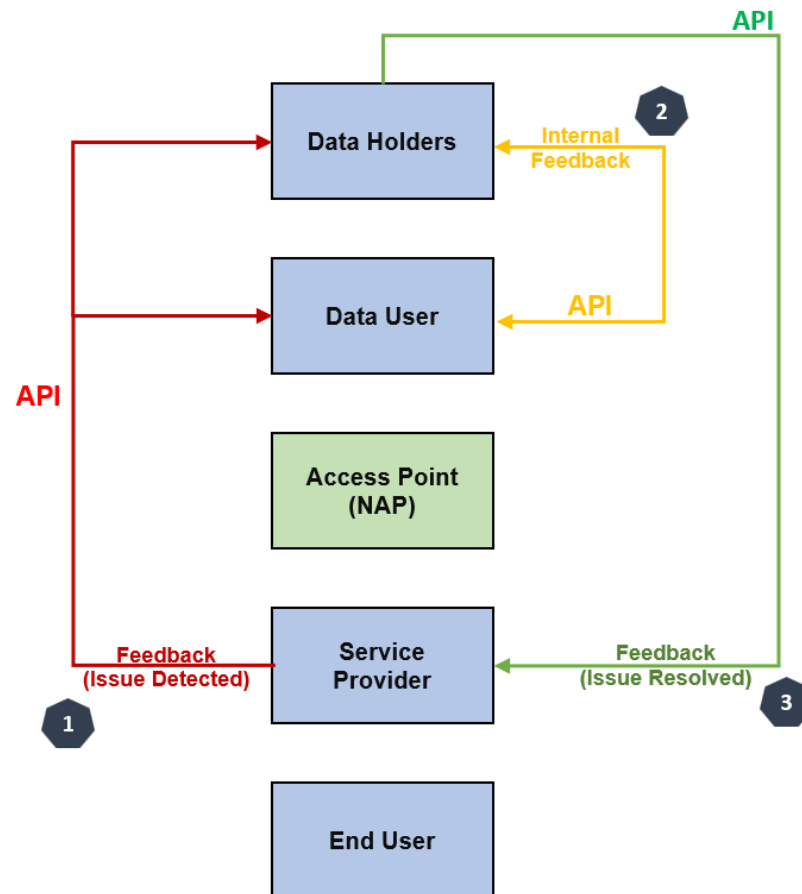


Figure 7 - Feedback Loop Scenario 2 Option I

- **Option II:** Service Provider feedback is directed towards the Access Point (NAP):
  - ✓ **Method:** In this approach, the feedback from the service provider is directed to an Access Point (NAP) via a special API (step 1). The NAP serves as an intermediary to manage the feedback.
  - ✓ **Processing the Feedback:** The Access Point can process the feedback by verifying the information received from multiple service providers and collating it into a structured format. This step ensures that the feedback is comprehensive, and any redundant or duplicate feedback is managed efficiently. The Access Point then forwards the verified and collated feedback to the data holder/data user using the special API (step 2). However, this means additional functionality needs to be implemented at the NAP. Upon receiving the feedback from the Access Point, the data holder/data user processes it (step 3), through internal feedback mechanisms, by analysing the information, verifying its accuracy, and determining any necessary actions to address the issues raised.
  - ✓ **Response to the Service Provider:** After processing, the data holder/data user can respond in two ways:
    - Response via Access Point (step 4): The data holder/data user responds to the Access Point, which then communicates the feedback and any

resolutions or updates to the respective service provider(s), completing the feedback loop.

- Direct Response (step 5): Alternatively, the data holder/data user responds directly to the service provider regarding the type of feedback, which completes the feedback loop.

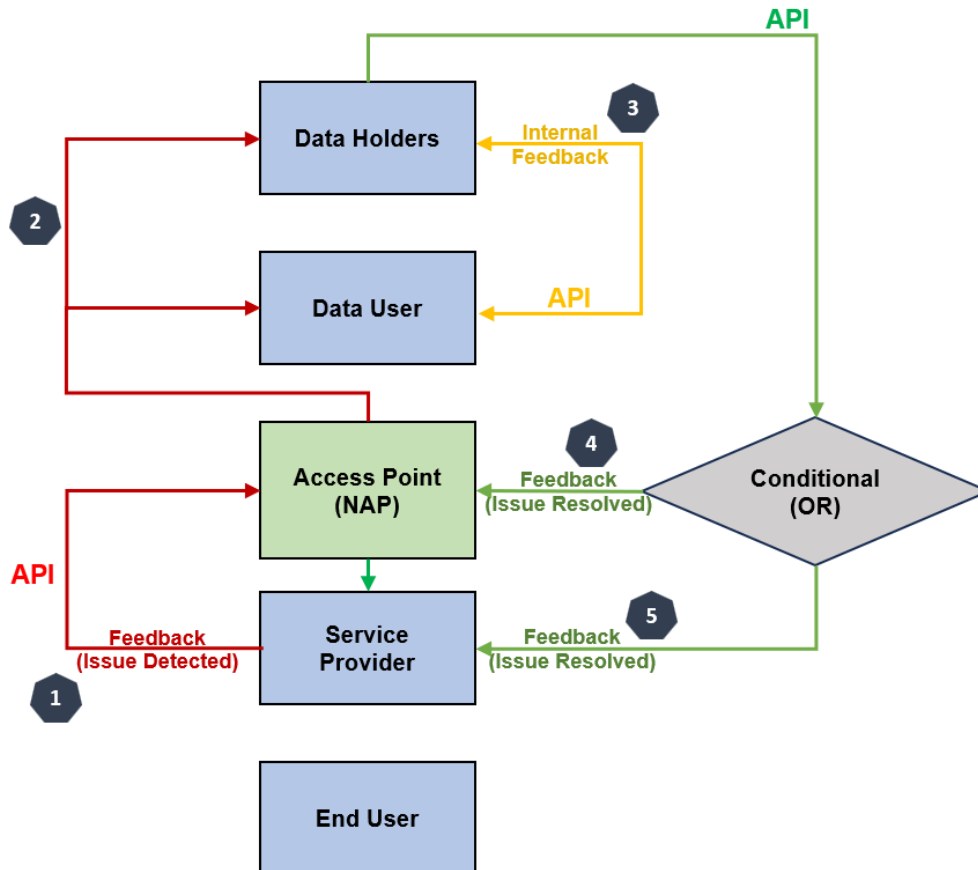


Figure 8 - Feedback Loop Scenario 2 Option II

Concerning the TISA report, the example of ISA speed limits, there are instances where the speed limit data for a road segment is available on a digital map, but many vehicles fail to capture the speed limit using their camera-based ISA systems. This situation can be an example of scenario 2, option I, where the service provider sends feedback to the data user and/or data holder, notifying them that an action may be necessary, whether fixing the speed limit sign or making it more visible to the road users. This approach aligns with the guidance provided by the CROW organisation in their released “Guidance for [Road Authorities on Intelligent Speed Assistance \(ISA\)](#)”<sup>46</sup>. Where CROW report highlighted the need for a feedback loop to the road authority in such cases to ensure swift response for the common good.

In both options from scenario 2, the feedback loop is designed to ensure effective communication and resolution of issues raised by service providers, enhancing the overall quality and reliability of the data and services provided.

<sup>46</sup> CROW, *Guidance for Road Authorities on Intelligent Speed Assistance (ISA)*, June 2021, [https://crowplatform.com/wp-content/uploads/2024/04/CROW\\_D503\\_EN\\_web-1-gecomprimeerd\\_2.pdf](https://crowplatform.com/wp-content/uploads/2024/04/CROW_D503_EN_web-1-gecomprimeerd_2.pdf)



**Internal Feedback: The Data User initiates a syntax feedback message**

The concept of an "Internal Feedback Loop", presented previously in all options of both scenarios, refers to a continuous cycle of communication and improvement between the Data User and the Data Holder. In this process, the Data User initiates a syntax feedback message, utilizing a specific use case where the feedback is directly shared with the Data Holder through a special API. Subsequently, the Data Holder processes the received feedback and responds to the Data User regarding the type of feedback processed, thus completing the loop. This internal loop is crucial for ensuring continuous improvements and data quality, fostering effective and efficient communication between the involved parties.

Internal feedback can also be initiated by the Data User without the involvement of the Service Provider or the End-User. In a real-world TN-ITS context, a practical example of an internal feedback loop might involve a scenario where a Data User, such as a national road authority, identifies discrepancies in the road attribute data provided by a Data Holder. For instance, the road authority might notice that several newly installed traffic signs, such as for speed limits, have not been updated in the central TN-ITS database.

**Note:** Other scenarios may exist but were not explored in depth due to their rarity.

Moreover, while this chapter outlines potential scenarios that a MS might encounter within this feedback loop, it is important to recognize that each MS operates under its unique circumstances. These differences arise from variations in governance structures, stakeholder relationships, regulatory frameworks, technological capabilities, and approaches to collaboration. Different gaps in NAPs of each MS can also play a crucial role. As a result, the methods for processing feedback and implementing changes can vary considerably between member states.

To apply the scenarios presented, each member state will need to carefully assess its specific context and make further adjustments to ensure the recommendations are suited to its own needs, challenges, and priorities. This approach helps ensure the feedback loop remains practical and relevant in each situation.

Furthermore, it is important to note that this milestone is not the only group working on tackling the issue of the feedback loop. For example, the RTTI Task Force conducted interviews with private service providers between June and October 2024 to produce their types of feedback loops (based on the interviews) and provide their reflections as well in the Debrief note they circulated on the 20<sup>th</sup> of January 2025<sup>47</sup>.

Their findings and conclusions from the interviews with the service providers have identified four different types of feedback loops, which can be consulted in the Debrief Note of the RTTI Task Force. Since the document is not yet publicly available, we have chosen not to list its conclusions in this report.

---

<sup>47</sup> RTTI Task Force, *RTTI Task Force Debrief note: Main Takeaways from Service Provider Interviews*, January 20, 2025



### 3.3.5. Challenges and Limitations

Implementing effective feedback loops within TN-ITS involves several challenges:

- **Stakeholder Resistance:** Resistance to new tools or processes can be mitigated by clearly communicating the benefits and providing training.
- **Technical Integration:** Integrating feedback tools with legacy systems requires careful planning and phased implementation.
- **Managing Feedback Volume:** Automated triage systems can help prioritize feedback, while human oversight ensures critical issues are addressed.
- **Resource Allocation:** According to the RTTI task force in September 2024, automatic real-time feedback and reporting on data improvements present potential challenges. They require significant resources from the Service Provider and often necessitate contract-based reimbursement.

As previously explained, possible tools for the feedback loop will be listed and presented in chapter 6 of this report, which will further complete this extensive analysis of the feedback loop.

### 3.4. TN-ITS Data-chain Updated Diagram

The TN-ITS data chain has undergone a significant evolution through successive milestones in different projects, reflecting the growing complexity and robustness required to manage the seamless flow of transportation-related data. This section provides a detailed account of this progression, from the initial linear model to the more comprehensive and dynamic circular approach now implemented.

In the early stages, as illustrated in the TN-ITS Go project and represented in the first diagram (Figure 9), the TN-ITS data chain was conceptualized as a linear process. This initial version featured five distinct stages: Data Collection, Data Processing, Data Exchange, Data Integration, and Data Usage. Each stage played a crucial role in ensuring that data, collected by road authorities and processed into standardized formats, could be exchanged, integrated, and ultimately used in various applications. While this model provided a clear framework for understanding the flow of data, it lacked mechanisms for continuous improvement and feedback.

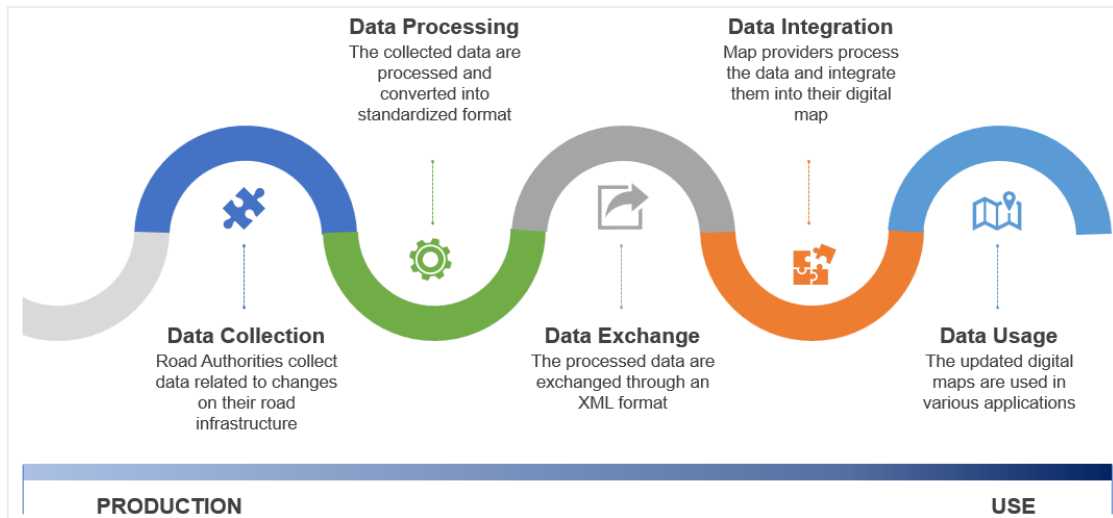


Figure 9 - Initial Linear TN-ITS Data Chain (Project TN-ITS Go)

Recognizing the limitations of the linear model, the TN-ITS data chain was reimaged as a circular process (Figure 10) in the subsequent phase, emphasizing the importance of feedback in maintaining the integrity and accuracy of the data. The circular model introduced in Milestone 4.2.6 added a sixth stage, the Feedback Loop, creating a continuous cycle of evaluation and refinement. This stage ensured that insights and corrections from each step could be fed back into the process, enhancing data quality and reliability across the entire chain.

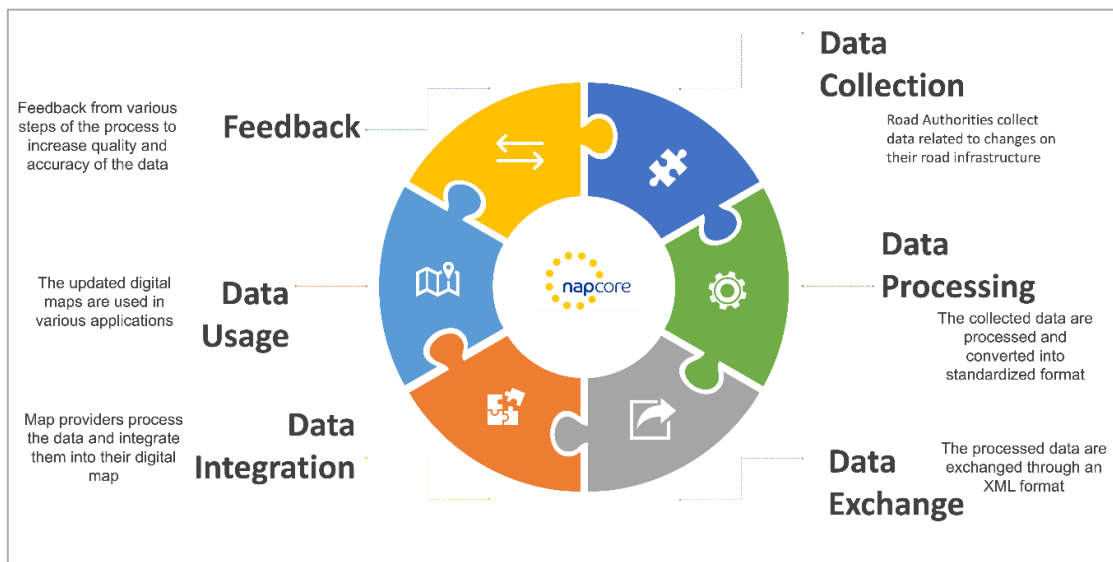


Figure 10 - Transition to a Circular Approach (Milestone 4.2.6)

In Milestone 4.2.7, the TN-ITS data chain diagram has been further refined to incorporate not only the five stages from previous models but also to integrate crucial roles (stakeholders) within the TN-ITS framework. This addition provided a full picture connecting individual roles/stakeholders with the particular stage in the chain diagram. A significant update in this version addresses feedback received on the circular model presented in Milestone 4.2.6,



where it appeared that the feedback loop was only active between the Data Collection and Data Usage stages. This was a misconception, and in this milestone, we have clarified that the feedback loop is indeed pervasive throughout the entire data chain, affecting all stages. This fact is supported by the premise that errors (intentional or unintentional) can arise at any stage of the data chain. Therefore, each stage should incorporate a feedback mechanism to identify and address inconsistencies effectively. This updated representation ensures that all stakeholders can contribute to and benefit from continuous improvements at every step of the process (Figure 11).

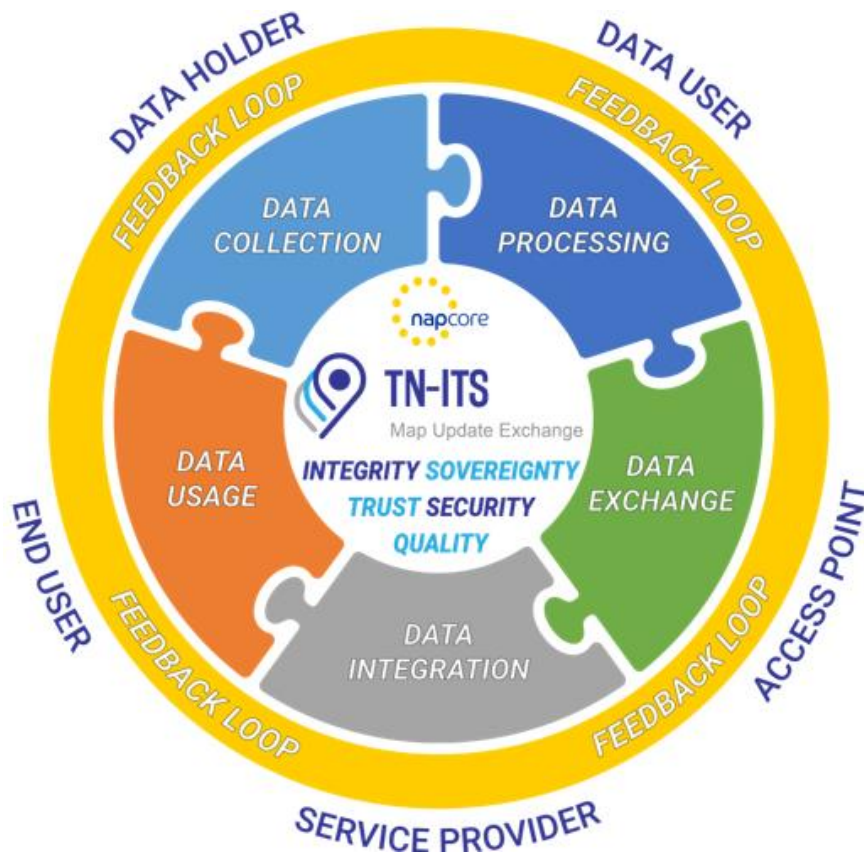


Figure 11 - The Latest Circular TN-ITS Data Chain with Enhanced Features (Milestone 4.2.7)

Additionally, this version emphasizes key data aspects (quality, trust, security, integrity, and sovereignty) while more carefully integrating the feedback loop across the data chain. This ensures a dynamic system where continuous evaluation and improvement are integral to the data management process.

This latest iteration represents a more sophisticated and interconnected system, where the circular approach is now enriched with an emphasis on interoperability and coordination within the broader mobility data ecosystem. By embedding the roles and responsibilities of various actors within the TN-ITS framework, this model provides a comprehensive, dynamic, and resilient structure that better supports the evolving demands of TN-ITS data management.

## 4. Critical evaluation of TN-ITS data chain processes

This chapter provides a comprehensive critical evaluation of the TN-ITS data chain processes, with a focus on the intricate relationships between the various stages of the TN-ITS data chain and the key data aspects of quality, trust, integrity, security, and sovereignty. This critical evaluation will provide valuable insights into the complex dynamics of TN-ITS data chain processes, offering actionable recommendations to enhance the system's overall efficiency, reliability, and security.

### 4.1. Data chain stages and data aspects analysis

A broad analysis was conducted to explore the potential impact. We distinguish 3 types of connection - **Direct**, **Indirect**, or **None** - between five critical data aspects and five stages of the TN-ITS data chain. The aim was to identify how these data aspects influence various stages of the data chain, without initially focusing on the specific roles of the different stakeholders involved. However, the findings from this generalized analysis proved inconclusive. This lack of clarity stemmed from the fact that, across nearly all stages and data aspects of the TN-ITS data chain, there was some level of direct involvement by various stakeholders, which blurred the distinct impacts we sought to identify. Consequently, this chapter sets the foundation for a more focused analysis by highlighting the complexities and challenges inherent in assessing these relationships on a broad scale.

Although the Feedback Loop is not considered a stage of the TN-ITS data chain, it has been included in this analysis to provide a more comprehensive understanding of the entire data chain.

	Quality (of Data)	Trust (Stakeholder)	Integrity (of Data)	Security	Sovereignty
<b>Data Collection</b>	Direct	Direct	Direct	Direct	Direct
<b>Data Processing</b>	Direct	Direct	Direct	Direct	Direct
<b>Data Exchange</b>	Direct	Direct	Direct	Direct	Direct
<b>Data Integration</b>	Direct	Indirect		Direct	Direct
<b>Data Usage</b>	Direct		Direct	Direct	
<b>Feedback Loop</b>	Direct	Direct	Direct	Direct	Direct

Table 5 - Impact between data aspects and data stages of the TN-ITS data chain

This task was challenging, as almost all stages are either directly or indirectly involved with these aspects. Despite these complexities, a solution was developed and is presented in the following section. Understanding these relationships remains essential to ensuring that the data processes maintain high standards of quality and reliability.

### 4.2. Mapping Stakeholder Responsibilities to Data Aspects

Building on the insights gained from the initial broad analysis, this chapter delves deeper into the relationships between roles and data stages within the TN-ITS data chain aspects by examining the potential impacts from the perspective of individual stakeholders. By analysing the specific roles that each stakeholder plays in the data chain, we were able to discern more

conclusive patterns of **direct** and **indirect** impacts (or none). This role-specific approach provided a clearer understanding of how different stakeholders interact with various stages of the data chain and how these interactions influence the overall quality, trust, integrity, sovereignty, and security of the data. The findings in this chapter offer a more detailed and accurate assessment, shedding light on the unique contributions and challenges associated with each stakeholder's involvement in the TN-ITS data ecosystem.

Quality (of Data)	Data Holders	Data Users	Access Point	Service Provider	End-User
Data Collection	Direct	Indirect			
Data Processing	Indirect	Direct			
Data Exchange		Direct	Indirect	Direct	
Data Integration				Direct	
Data Usage				Indirect	Direct
Feedback Loop	Direct	Direct	Indirect	Direct	Direct

Table 6 - Stakeholder Impact on data stages for Quality (of data) aspect

**Quality analysis output:** The quality of data is most influenced by direct interactions at the data collection stage and the feedback loop, where Data Holders and Data Users play critical roles. The feedback loop stands out with multiple stakeholders, including Data Holders, Data Users, Service Providers, and End-Users, all directly contributing, which highlights the importance of continuous feedback in maintaining and enhancing data quality throughout the TN-ITS data chain. This indicates that a collaborative approach during these stages is vital for ensuring high data quality.

Trust (on Stakeholder)	Data Holders	Data Users	Access Point	Service Provider	End-User
Data Collection	Direct	Direct			
Data Processing	Direct	Direct			
Data Exchange		Direct	Indirect		
Data Integration				Indirect	
Data Usage					
Feedback Loop	Direct	Direct	Indirect	Direct	Direct

Table 7 - Stakeholder Impact on data stages for Trust (on stakeholder) aspect

**Trust analysis output:** Trust on stakeholders is predominantly established through direct interactions during the data collection, processing, and exchange stages, and feedback loop. Both Data Holders and Data Users consistently engage directly in most of these phases, which suggests that their active participation is essential for fostering trust within the TN-ITS data chain. The feedback loop with direct involvement from multiple stakeholders, underscores its critical role in sustaining trust across the entire process.

Integrity (of Data)	Data Holders	Data Users	Access Point	Service Provider	End-User
Data Collection	Direct	Direct			
Data Processing	Indirect	Direct			

<b>Data Exchange</b>		Direct	Indirect	Direct	
<b>Data Integration</b>					
<b>Data Usage</b>					Direct
<b>Feedback Loop</b>		Direct		Direct	Direct

Table 8 - Stakeholder Impact on data stages for Integrity (of data) aspect

**Integrity analysis output:** Data integrity is most strongly upheld through direct engagement during the data collection, processing, and exchange stages, and feedback loop, where both Data Holders and Data Users are key players. The feedback loop is especially crucial, with direct contributions from multiple stakeholders, ensuring that any discrepancies are identified and corrected, thereby maintaining the integrity of the data over time. This emphasizes the importance of continuous oversight and collaboration to protect data integrity.

<b>Security (on Data and Exchange)</b>	<b>Data Holders</b>	<b>Data Users</b>	<b>Access Point</b>	<b>Service Provider</b>	<b>End-User</b>
<b>Data Collection</b>	Direct	Direct			
<b>Data Processing</b>	Direct	Direct			
<b>Data Exchange</b>		Direct	Indirect	Direct	
<b>Data Integration</b>				Direct	
<b>Data Usage</b>					Direct
<b>Feedback Loop</b>				Direct	Direct

Table 9 - Stakeholder Impact on data stages for Security (on Data and Exchange) aspect

**Security analysis output:** Data security is primarily reinforced through direct involvement during the data collection, processing, and data exchange stages. The Data Users and the Service Providers play pivotal roles. This multi-stakeholder engagement at critical points of the data chain underscores the need for a robust and collaborative approach to securing data throughout its lifecycle.

<b>Sovereignty (over the Data)</b>	<b>Data Holders</b>	<b>Data Users</b>	<b>Access Point</b>	<b>Service Provider</b>	<b>End-User</b>
<b>Data Collection</b>	Direct				
<b>Data Processing</b>		Direct			
<b>Data Exchange</b>		Direct	Indirect	Direct	
<b>Data Integration</b>				Direct	
<b>Data Usage</b>					
<b>Feedback Loop</b>	Direct	Direct		Direct	Direct

Table 10 - Stakeholder Impact on data stages for Sovereignty (over the Data) aspect

**Sovereignty analysis output:** Data sovereignty is largely maintained through direct involvement in the data collection and data exchange stages, and the feedback loop. Data Holders and Data Users are consistently directly involved in these phases, particularly in the feedback loop, where sovereignty is reaffirmed by multiple stakeholders. The significant number of direct interactions in these stages indicates that ensuring sovereignty requires a

proactive approach to managing and overseeing data control, especially as it moves through different hands within the TN-ITS data chain.

### 4.3. Data aspects overlapping analysis

In the context of the TN-ITS data chain, understanding the intricate relationships between various data aspects such as Data Quality, Trust, Data Integrity, Data Security and Data Sovereignty is crucial for optimizing the overall effectiveness and reliability of the system. However, these relationships are not always straightforward, and the influence one aspect may have on another can vary in strength and direction.

This analysis was designed to provoke a critical discussion and numerically quantify relations between these aspects. To approach this systematically, a structured scoring system was implemented which was done based on expert's opinion and their in-depth understanding of the TN-ITS data chain concept. The analysis seeks to explore the bidirectional relationships between these data aspects, providing a critical evaluation of how each one potentially influences the others. The initial assessments offered an optimistic view, suggesting strong interdependencies. However, upon closer inspection, these connections often involve multiple factors, and the impact is not always direct or guaranteed.

Given the inherent complexity and occasional overlap between these data aspects, even when the connections are highly indirect, a decision was made to quantify these relationships using a scoring system ranging from 1 to 10.

- A score of **1 (one)** represents a **very indirect relationship**.
- A score of **10 (ten)** implies a **very direct relationship**.

The revised scores and explanations presented here offer a more nuanced and realistic assessment of these relationships within the TN-ITS data chain. By acknowledging the complexity and variability of these interactions, this analysis provides a more measured and accurate understanding of how these data aspects overlap and influence each other, helping stakeholders make informed decisions in managing and optimizing their data processes.

This analysis is designed to provoke thoughtful discussions and raise critical questions about these scenarios, acknowledging that there is no one-size-fits-all approach for all stakeholders, including Member States, due to the vastly different circumstances they each encounter. The goal is to encourage a more in-depth exploration and debate on how the overlaps between these data aspects manifest in real-world settings, while fully recognizing the complexity and variability that exists across diverse contexts.

	Quality (of Data)	Trust (on Stakeholder)	Integrity (of Data)	Security (on Data)	Sovereignty (over the Data)
Quality (of Data)		9	10	1	4
Trust (on Stakeholder)	4		4	6	4
Integrity	10	8		7	7



(of Data)					
Security (on Data)	3	8	9		9
Sovereignty (over the Data)	3	6	4	7	

Table 11 - Relationship between the TN-ITS data chain data aspects

#### i. Data Quality and Trust

Improving Data Quality Enhances Trust: High-quality data generally increases trust among stakeholders because it reduces uncertainty and supports reliable decision-making. However, trust also depends on other factors, such as historical performance and external influences, meaning that the improvement in trust might not be automatic or guaranteed. - **Score: 9**

Increased Trust on stakeholders improves Data Quality: While trust can encourage stakeholders to contribute more diligently, this is not guaranteed. Stakeholders might still prioritize other factors, such as cost or convenience, over quality, even if they trust the system. - **Score:4**

#### ii. Data Quality and Data Integrity

Improving Data Quality enhances Data Integrity: High-quality data that is consistent and reliable naturally supports data integrity, as it minimizes the chances of discrepancies or errors. This relationship is strong because both concepts are closely related. - **Score: 10**

Increased Data Integrity improves Data Quality: When data integrity is maintained, it directly preserves the quality of the data by ensuring it remains unaltered and consistent, reinforcing their close connection. - **Score: 10**

#### iii. Data Quality and Data Security

Improving Data Quality enhances Data Security: While good quality data might help in setting appropriate security measures (e.g., precise access controls), the connection is not direct. Security is more about protection mechanisms than about data quality per se. - **Score: 1**

Increased Data Security improves Data Quality: Security measures help protect the data from unauthorized alterations, thus indirectly preserving its quality. However, security measures alone do not guarantee high data quality unless they are specifically designed to support quality assurance. - **Score: 3**

#### iv. Data Quality and Data Sovereignty

Improving Data Quality enhances Data Sovereignty: High-quality data can make it easier for stakeholders to enforce and maintain their sovereignty by providing accurate information for decision-making and control. However, data sovereignty also heavily relies on legal and procedural frameworks, not just quality. - **Score: 4**

Increased Data Sovereignty improves Data Quality: When stakeholders have strong control over their data, they can enforce quality standards more effectively. However, sovereignty mainly ensures control rather than directly improving quality, which still depends on the practices and resources dedicated to quality assurance. - **Score: 3**

#### v. Trust and Data Integrity

Improving Trust enhances Data Integrity: Trust in the systems and processes used to maintain data integrity can lead to better adherence to best practices. However, trust does not automatically result in improved integrity; it requires that trusted processes are also robust. -

**Score: 4**

Increased Data Integrity improves Trust: Strong data integrity helps build trust by ensuring data is reliable and unaltered. This relationship is strong, as trust is closely tied to the assurance that data is intact and reliable. - **Score: 8**

#### vi. Trust and Data Security

Improving Trust enhances Data Security: Trust in security systems can lead to better compliance with security protocols but trust alone does not ensure that all stakeholders will follow best practices. Compliance also depends on enforcement and the perceived importance of security. - **Score: 6**

Increased Data Security Improves Trust: Effective security measures directly build trust by protecting data from breaches and unauthorized access, leading to a strong relationship.

- **Score: 8**

#### vii. Trust and Data Sovereignty

Improving Trust Enhances Data Sovereignty: Trust in data handling practices can reinforce perceptions of sovereignty, but this is more about perception than a direct enhancement of sovereignty. The actual control over data (sovereignty) depends more on legal frameworks and enforcement. - **Score: 4**

Increased Data Sovereignty improves Trust: When stakeholders feel their control over data is respected and enforced, it can build trust. However, this trust depends on consistent and fair application of sovereignty rules, so the connection is not absolute. - **Score: 6**

#### viii. Data Integrity and Data Security

Improving Data Integrity enhances Data Security: Ensuring data integrity contributes to security by preventing unauthorized changes. However, data security involves more than just integrity, such as access controls and encryption, making this connection strong but not total.

- **Score: 7**

Increased Data Security improves Data Integrity: Security measures, like encryption and access controls, directly protect data integrity by preventing unauthorized changes. This relationship is quite strong. - **Score: 9**

#### ix. Data Integrity and Data Sovereignty

Improving Data Integrity enhances Data Sovereignty: Maintaining data integrity supports data sovereignty by ensuring that the data remains true to its original form, but sovereignty is also about control and legal rights, not just integrity. - **Score: 7**

Increased Data Sovereignty improves Data Integrity: Strong control over data can help ensure its integrity by allowing stakeholders to enforce rigorous standards. However, sovereignty doesn't automatically lead to high integrity; it depends on how that control is used. - **Score: 4**

#### x. Data Security and Data Sovereignty



Improving Data Security enhances Data Sovereignty: Secure data handling helps ensure that an entity maintains control over its data, supporting data sovereignty. This connection is strong, as security measures are a key component of maintaining sovereignty. - **Score: 9**

Increased Data Sovereignty improves Data Security: When stakeholders have control over their data, they are more likely to implement strong security measures, but sovereignty alone doesn't ensure security unless it is actively enforced. - **Score: 7**



## 5. Optimal TN-ITS Data-Chain Framework

The TN-ITS data chain represents a complex ecosystem encompassing various critical dimensions such as data quality, trust, security, integrity, and sovereignty. Each of these data aspects plays a pivotal role in ensuring the reliability and effectiveness of the TN-ITS framework. This chapter explores the multi-dimensionality of such a framework, comprising independent yet interconnected components aimed at enhancing the overall quality and trustworthiness of TN-ITS data.

The methodology agreed upon, in this section, by Task Group 4.2.4 was to first explore the vulnerabilities, limitations, concerns, and potential issues associated with implementing such a comprehensive framework and propose strategies and solutions, such as countermeasures, to effectively address these challenges. All these suggestions and guidelines will then contribute to shaping a potential optimal TN-ITS data chain framework based on the five data aspects under study.

### 5.1. Potential vulnerabilities, attacks, and countermeasures (Update)

This section provides an updated overview of the vulnerabilities within the TN-ITS data system and the corresponding countermeasures needed to address them, building upon the findings of Milestone 4.2.6. It begins by outlining targeted strategies to mitigate key vulnerabilities across the TN-ITS data chain stages. Next, it assesses the impact of these vulnerabilities based on the critical importance of trust, quality, security, integrity, and sovereignty in maintaining a secure and reliable data system. The analysis also identifies the tasks and responsibilities of key stakeholders (roles), in implementing these countermeasures. Finally, it digs into security and integrity-related vulnerabilities, emphasizing the need for a risk-based approach to cybersecurity.

#### 5.1.1. Targeted Countermeasures: Addressing Vulnerabilities

Main Vulnerability	Secondary Vulnerabilities	Potential Countermeasures
<b>Incorrect data input</b> (Data Collection)	Data tampering	Implement strong data authentication mechanisms to detect unauthorized modification. Use digital signatures or cryptographic hashing to ensure data integrity and prevent tampering.
	Human Error	Regular training of personnel to minimize human errors.
	Sensor inaccuracies (outdated equipment, failure and/or malfunction)	Regular maintenance and updating of sensor equipment and frequent calibration of sensors to ensure accuracy.
	Phishing/Nefarious activity or abuse	Security awareness training to identify and avoid phishing attacks. Implement multi-factor authentication to protect access.
	Inadequate coverage	Conduct coverage studies to identify areas with inadequate coverage. Invest in technology to expand coverage where necessary.

	Data provenance	Implement a data provenance tracking system to ensure the authenticity of data sources. Regularly audit the data custody chain.
<b>Incorrect processes or data values</b>  (Data Processing)	Algorithmic biases	Regularly audit algorithms to detect and correct biases. Use diverse and balanced datasets for algorithm training.
	Erroneous data transformations	Implement a multi-stage validation process to detect and correct inconsistencies with regular review and audit data transformations to ensure accuracy.
	Supply-chain attacks	Continuously monitor suppliers to detect early signs of attacks. Conduct cybersecurity assessments and regular security audits of suppliers.
	Inadequate data anonymization techniques	Adopt robust data anonymization techniques such as k-anonymity, l-diversity, or differential privacy. Regularly test anonymization methods to ensure that data cannot be reidentified.
	Computational resource limitations	Implement resource monitoring tools to identify and mitigate bottlenecks. Plan and allocate sufficient computational resources for peak processing times.
<b>Malicious Data Injection</b>  (Data Exchange)	Unauthorized access	Implement strict access controls and multi-factor authentication to prevent unauthorized access by regularly monitoring and log access attempts to detect suspicious activities.
	Data leakage	Encrypt data both in transit and at rest to safeguard it from leakage. Implement Data Loss Prevention (DLP) tools and monitor for potential leaks.
	Malware	Deploy advanced malware detection and prevention systems, including endpoint protection solutions. Regularly update and patch systems to mitigate vulnerabilities.
<b>Lack of standardization</b>  (Data Exchange)	Insecure Transmission Protocols	Use secure transmission protocols such as TLS/SSL to protect data exchange. Conduct regular security testing, including penetration tests, to identify and resolve protocol vulnerabilities.
	Outdated metadata	Establish and enforce metadata standards across the stakeholders. Regularly review and update metadata to ensure it remains current and consistent.
	Inconsistent metadata	Implement a centralized metadata management system to maintain consistency. Perform regular audits to identify and correct metadata inconsistencies.
<b>Incorporating wrong data into the maps</b>  (Data Integration)	Data compatibility issues	Implement rigorous data validation processes to detect compatibility issues. Use middleware solutions to facilitate interoperability between different systems and formats.
	Conflicting data schemas	Standardize data schemas across the stakeholders to prevent conflicts. Regularly audit and harmonize data schemas to ensure alignment.
	Poor data mapping techniques	Use standardized data mapping practices and tools and continuously review and refine data mapping techniques to enhance accuracy.
	Semantic heterogeneity	Develop and implement ontologies and data dictionaries to ensure semantic alignment across systems and utilize

		semantic integration tools that support automatic mapping and translation of data semantics.
<b>Display false or wrong information</b>  (Data Usage)	Data misinterpretation	Provide user training and clear documentation on correct data interpretation practices. Implement data visualization tools that highlight uncertainties and provide context.
	Improper utilization of context	Implement decision support tools that correctly integrate and present contextual data.
	Biased decision-making	Regularly audit decision-making processes to identify and mitigate bias.
	Lack of User Training	Develop comprehensive, ongoing training programs for users to ensure they are equipped to use data correctly. Regularly assess and update training materials to cover emerging challenges and knowledge gaps.
	Misleading Visualizations	Validate all visualizations for accuracy and clarity before they are shared with end-users.
	Denial-of-service (DoS, DDoS)	Deploy DDoS mitigation services and scalable infrastructure to handle high traffic volumes. Monitor network activity continuously to detect and respond to DoS attacks promptly.
	Ransomware attacks	Maintain regular, secure backups of critical data to enable quick recovery from ransomware attacks. Implement comprehensive cybersecurity measures, including next-gen firewalls and anti-ransomware tools.
	Lack of transparency	Establish and communicate a clear data transparency policy to users. Use transparency tools that allow users to trace data origins and understand data limitations.

Table 12 - Vulnerabilities in the TN-ITS Data Chain and Potential Countermeasures

### 5.1.2. Vulnerabilities Impact Assessment and Critical Data Aspects

This section provides an analysis of the impact across various stages of the TN-ITS data chain, identifying key vulnerabilities and emphasizing the importance of critical data aspects such as trust, quality, security, integrity, and sovereignty.

**Note:** For detailed analysis and results, refer to Annex B.

The process for evaluation, in Annex B, was created by measuring the integration of each data aspect into the vulnerability clustering. Specifically, it was agreed that the values given would reflect as such:

- A value of 1 represents **full integration**
- A value of 0.5 represents **partial integration**
- A value of 0 represents **no integration**

In the following analysis are the percentages of the impact integration according to the values presented in Annex B.



- **Impact by Data Chain Stage** (which data chain stages are most or least impacted by the suggested vulnerabilities):
  - Data Collection (Impact: 73%): This stage shows a significant potential for impact due to the foundational nature of this phase. Any issues or vulnerabilities at this point can ripple through the entire data lifecycle, compromising all subsequent stages. The score reflects the critical importance of ensuring that data is accurate and reliable from the start. Errors in data collection can undermine trust and reduce the overall quality of the data, which is crucial for all later processes.
  - Data Processing (Impact: 72%): This stage is also highly susceptible to impact. At this stage, raw data undergoes various transformations and standardizations, which are crucial for making it usable. If vulnerabilities occur here, they can distort the data's integrity, leading to inaccuracies that affect decision-making and other downstream applications. The high impact score highlights the necessity of rigorous processing protocols to maintain the integrity and quality of the data.
  - Data Exchange (Impact: 90% for Malicious Data Injection; 87% for Lack of Standardization): This stage is particularly vulnerable, as indicated by the highest impact scores. This phase involves the transfer of data between systems or entities, making it susceptible to security breaches and inconsistencies. Any disruption here can have severe consequences, compromising the entire data system. The high impact reflects the importance of secure and standardized data exchange processes to prevent any potential threats that could lead to data corruption or loss.
  - Data Integration (Impact: 80%): This stage shows a significant impact potential as well. This phase is where data from different sources is combined, which can introduce compatibility issues or discrepancies if not handled properly. A high impact score here emphasizes the critical role of accurate data integration in ensuring that the final dataset remains consistent, reliable, and true to the sources.
  - Data Usage (Impact: 75%): This stage is also highly impacted by vulnerabilities. This is the stage where data is applied for decision-making or other practical uses, as well as data being utilised in traffic situations to improve road safety, making it crucial that the data is accurate and trustworthy. Any issues at this stage can lead to incorrect conclusions and poor decisions. The high impact score underlines the need for careful handling and interpretation of data to avoid significant negative outcomes.
  
- **Impact by Data Aspect** (which data aspect is most or least critically impacted by the suggested vulnerabilities):
  - Trust (Impact: 95%): Trust is one of the most critical aspects across all stages, reflecting its fundamental role in the data chain.
  - Quality (Impact: 88%): Quality is highly important whereas maintaining high-quality data is crucial.
  - Integrity (Impact: 97%): Integrity scores the highest importance highlighting its criticality in ensuring data is accurate and reliable.
  - Security (Impact: 64%): Security, while still important, is less critical compared to trust, quality, and integrity, showing a more moderate but necessary impact.

- Sovereignty (Impact: 45%): Sovereignty has the least importance, although still relevant, particularly in stages involving cross-border data exchange or when data provenance is critical.

### 5.1.3. Identifying Key Stakeholders for Countermeasure Implementation

This analysis highlights the distributed nature of responsibilities across different stakeholders in the data chain.

**Note:** For detailed analysis and results, refer to Annex C.

The process for the evaluation, in Annex C, was created by measuring the level of responsibility that each stakeholder has for implementing a countermeasure. The values that were used were agreed that would be reflected as such:

- A value of 1 represents **full responsibility**
- A value of 0.5 represents **partial responsibility**
- No value represents **no responsibility**

In the following analysis are the percentages of major stakeholders' responsibility according to the values presented in Annex C.

- **Data Holders (61% Responsibility)**
  - High Responsibility Stage: The Data Collection and Data Processing stages demand the most from Data Holders, where they need to ensure data accuracy, prevent errors, and maintain data quality through robust validation and maintenance processes.
  - Lower Responsibility Stage: Their role is less intensive in the Data Usage stage.
- **Data Users (75% Responsibility)**
  - High Responsibility Stage: The Data Usage stage sees Data Users taking on the most significant role, where they must correctly interpret and apply the data, avoiding misinterpretations and biases.
  - Lower Responsibility Stage: Their responsibility is less critical during the Data Usage stage.
- **Access Points (55% Responsibility)**
  - High Responsibility Stage: The Data Exchange stage is where Access Points are most heavily involved, as they are responsible for ensuring the secure transmission of data and protecting it from potential threats during exchanges.
  - Lower Responsibility Stage: Their involvement is minimal in the Data Collection and Data Processing stages.
- **Service Providers (54% Responsibility)**
  - High Responsibility Stage: Service Providers are most critical during the Data Integration and Data Usage stage, where they must provide reliable tools and infrastructure to facilitate correct data usage and prevent issues like DoS attacks or ransomware.

- Lower Responsibility Stage: Their responsibility is lower in the Data Collection and Data Processing stages.
- **End Users (0% Responsibility)**
  - N/A – End Users are not typically responsible for implementing countermeasures. Across all stages, End Users are primarily focused on utilizing the data rather than managing or securing it.

### 5.1.3.1. Analysis of Security and Integrity-Related Identified Vulnerabilities

System implementing TN-ITS specifications require a high level of cybersecurity, which, however, should follow the proportionality approach: risk analysis is driving the implementation and the nature of the countermeasures. On the other hand, TN-ITS systems shall be interoperable, and interoperability is a key aspect of Availability, as part of the CIA (Confidentiality, Integrity, Availability) triad<sup>48</sup>, identified in ISO 27001:2022. A lack of interoperability hinders the availability of the TN-ITS service.

Risk analysis is an aspect that is driven by the context in which the system is developed, operated, and decommissioned. As examples, we may have the following cases:

- Development stage: code can be poisoned<sup>49</sup>, both open-source and closed-source libraries may be outdated and exploitable, or attackers may compromise continuous delivery systems.
- Operation stage: the system may be executed in untrusted boundaries (vulnerable or misconfigured operating system, untrusted cloud provider), the system may be a target of a DDoS attack, or under several Advanced Persistent Threats (APT)
- Decommission stage: the system may be removed from operation in an insecure way so that secrets, private keys, and connection strings are exposed.

Systematically addressing all the threats is impossible. However, to provide a minimum baseline of cybersecurity, frameworks have been proposed. The most prominent one is the MITRE ATT&CK Framework<sup>50</sup>. This framework created a taxonomy of tactics based on existing exploitation techniques and allows the reasonings for creating a *threat model*. According to OWASP<sup>51</sup>, threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting the TN-ITS service.

At this stage, it is premature to identify who may be the eventual opponents to the TN-ITS services. They may be state-sponsored, hackers, or ransomware gangs. External bodies

<sup>48</sup> RIGCert, *ISO/IEC 27001-12*, last accessed January 2025, [https://www.rigcert.org/iso\\_iec\\_27001-12.htm#:~:text=Information%20security%20is%20commonly%20defined,information%20when%20they%20need%20it](https://www.rigcert.org/iso_iec_27001-12.htm#:~:text=Information%20security%20is%20commonly%20defined,information%20when%20they%20need%20it).

<sup>49</sup> Lasse Collin, XZ Utils backdoor, last updated January 2025, <https://tukaani.org/xz-backdoor/>, last accessed January 2025

<sup>50</sup> MITRE, *ATT&CK*, last accessed January 2025, <https://attack.mitre.org>,

<sup>51</sup> Drake Victoria, *Threat Modeling*, last accessed January 2025, [https://owasp.org/www-community/Threat\\_Modeling](https://owasp.org/www-community/Threat_Modeling),



such as ENISA regularly publish reports, named *threat landscape*<sup>52</sup>. Recently, ENISA promoted the threat landscape for the transport sector (ENISA TLT).

Those two assets, the threat landscape and the MITRE ATT&CK are used as a basis for the definition of the cybersecurity requirements of the TN-ITS service. However, it is worth noting that this deliverable will provide the minimum set of requirements to attain interoperability. Each company running the services must perform an internal business impact analysis and risk assessment to further protect the system.

According to the ENISA TLT, the following threats have been identified:

- Ransomware attacks
- Data related threats
- Malware
- Denial-of-service, distributed denial-of-service, ransom denial-of-service
- Phishing
- Supply-chain attacks

Most of the threat categories fall in the operation stage. Protecting from ransomware attacks, malware, DDoS, phishing, or supply-chain attacks pertains to the organization running the TN-ITS systems: TN-ITS provide only interoperability specifications. However, data-related threats are still in focus. Data leakage, malicious access to classified data, unavailability of data, and loss of integrity are threats observed by the TLT.

In conclusion, TN-ITS should consider the future creation of a threat model that incorporates data-related threats as input. This model would utilize the standard Confidentiality-Integrity-Availability analysis to outline the security countermeasures defined in the next section.

## 5.2. TN-ITS security and integrity

TN-ITS is an End-User driven standardized data sharing platform, with a focus on the exchange of map attribute updates between road authorities and digital map service providers. The TN-ITS framework includes a standardized data format and protocols for data exchange, ensuring compatibility and interoperability between different systems and stakeholders.

As a result of extensive discussions within the group, it was determined that the aspects of security and integrity would be maintained at a more general level, while greater emphasis would be placed on quality and trust. This section represents the outcome of these deliberations, which also contributed to the identification of potential tools, relevant to these data aspects, that will be expanded upon in section 6 of this report.

TN-ITS stakeholders are defined throughout its data chain, and they are as follows (contextualized for cybersecurity):

---

<sup>52</sup> ENISA, *Threat Landscape*, last accessed January 2025, <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends>,



- Data Users and Data Holders are responsible for generating and supplying accurate and reliable data related to traffic and navigation.
- Access Points (e.g., the NAP), are responsible for facilitating the exchange and distribution of data within the TN-ITS data chain.
- Service Providers are stakeholders that utilize the data available in the TN-ITS data chain to provide services and applications for the End-Users.

Establishing security checks in the TN-ITS ecosystem is a multidimensional task. The following aspects have been considered:

- Authorization
- Authentication
- API Security (and clock synchronization)
- Integrity
- Sovereignty

Other aspects of security, in addition to the one mentioned in the previous section such as brand recognition, also have ICT aspects that are out of the scope of this document. For instance, company security policies or Cyber Threat Intelligence can increase the Brand Reputation by observing the public exposure of vulnerable services.

### 5.2.1. Approach for ensuring suitable security and integrity mechanism

The security and integrity of TN-ITS are defined in terms of ABB (Architectural Building Blocks) and IBB (Information Building Blocks), which serve as fundamental components in structuring and securing data exchanges. ABBs define high-level system functionalities, while IBBs focus on managing and protecting the information itself. Each ABB specifies a set of MITRE ATT&CK techniques, tactics, and relevant data sources that it addresses.

As established in previous analyses, TN-ITS data requires authorization or a threat model. Therefore, it must be protected during transmission and delivered through designated Access Points that expose secure APIs (e.g., a NAP). Similarly, data integrity must be ensured and safeguarded throughout the entire data chain.

Examples of ABBs are as follows:

- Authorization ABB: define a means to protect the data in transit through authorization tokens (e.g., technologies such as OpenID or SAML).
- Node Authentication ABB: define a means to authenticate the node (e.g., the host, the application service, or the microservice) through TLS 1.2 and 1.3.
- Data Encryption ABB: defines a means to encrypt data (or part of it) while at rest and in transit, through standards such as XML Encryption.
- Non-Repudiation ABB: define several ways of non-repudiation (origin, destination, submission, delivery), based on ISO 13888.
- Data Integrity ABB: define a way to sign messages, through XML or JSON Digital Signature.

- Data Provenance ABB: define a way, based on W3C PROV, to track the provenance of data, when data is created, and when data is modified.

### 5.3. TN-ITS trust

The definition of trust is multifaceted. Trust is a relationship that is established on multiple aspects (e.g., technological, legal, organizational) and levels (e.g., interoperability of services, quality of the data). Principle 8 of the European Interoperability Framework (EIF)<sup>53</sup>, states that “Citizens and businesses must be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment”, with recommendation 15 “Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and interactions with citizens and business”. As TN-ITS aims to provide a standard and interoperable methodology in its value chain, the EIF interoperability levels must be considered. A concise, agreed upon definition of trust is presented in Chapter 2 and forms the basis of this work.

To establish trust between the TN-ITS Data chain, it needs to be simultaneously tackled at the different EIF interoperability layers, which are legal, organisational, semantic, and technical. This section briefly touches upon the technical aspect of ensuring trust while the focus resides on the organisational aspect.

#### 5.3.1. Technical Approach for Ensuring Suitable Trust Mechanism

From a technical perspective, most of the trust-enabling measures either process or technology, are based on the context in which the TN-ITS systems are running. Cybersecurity plays a vital role in establishing trust, but Cybersecurity measures are identified by mitigating risks and known vulnerabilities: this is the reason why Cybersecurity measures are defined upon context-dependant building blocks, whose adoption is driven by risk analysis.

Adopting the ABBs and IBBs introduce a governance aspect of trust which must be driven by risk analysis. The NAPCORE Reference Architecture Model for Security and its Building Block deliverable will provide an approach to ensure the interoperability of secure architecture for TN-ITS, based on a STRIDE threat model<sup>54</sup>, to be further developed in the governance parts by each organization.

It is worth noting that in other verticals, trust is established through security policy. For instance, the C-ITS Security Policy defined by the CPOC<sup>55</sup> realizes the trust among the

---

<sup>53</sup> European Commission, *European Interoperability Framework*, last September 2024, [https://ec.europa.eu/isa2/sites/isa/files/eif\\_brochure\\_final.pdf](https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf)

<sup>54</sup> Learn-Microsoft, *Microsoft Threat Modeling Tool threats*, August 2022, <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model>

<sup>55</sup> European Commission, *C-ITS Point of Contact*, last accessed January 2025, <https://cpoc.jrc.ec.europa.eu/>



stakeholders through ISO 27001:2022. Each ABB is mapped to specific ISO 27001:2022 controls, detailing the measures it implements and how they can serve as evidence for an external audit. However, ISO 27001:2022 is not deemed necessary by TN-ITS data users as the situation of the NAP's role in the system of high criticality according to the EU 2022/2555 (the NIS 2) has not yet been streamlined by the national authorities. Therefore, it is premature to require systems to implement an Information Security Management System (ISMS) certified according to ISO 27001:2022 as it may be superseded by the NIS 2 obligations. Eventually, this approach may be revised when the national authorities provide a final statement on the NAP's role in systems with high criticality, by eventually proposing an ISO 27001:2022-based framework for attaining trust.

Another standard to be considered is the ISO/IEC TR 24028:2020. This standard provides comprehensive guidance on achieving transparency, explainability, and controllability in AI systems, which are crucial for maintaining stakeholder trust. Therefore, all data evaluation tools deployed must include mechanisms to assess these aspects in alignment with ISO/IEC TR 24028:2020. Since AI-capable systems are a concept that can and should be integrated into most of the tools listed here, it was decided not to create a specific tool for AI but to consider its possible integration into all of them during implementation.

An additional crucial standard for ensuring trusted data exchanges is CWA 18125:2024, which sets out guidelines for trusted data transactions and is essential in addressing the vulnerabilities identified in the TN-ITS data chain. By adopting these guidelines, the TN-ITS system can ensure that all data transactions are conducted with a high degree of trust and security, thereby minimizing the risk of data breaches or unauthorized access. This approach enhances the overall security posture of the TN-ITS data chain by embedding trust at the core of data exchanges, making the system more resilient against potential cyber threats.

Some of the guidelines provided by the CWA 18125:2024 reinforce certain countermeasures listed earlier in this report. Examples include implementing strong authentication and authorization mechanisms, establishing data integrity checks, regular audits and monitoring, adopting end-to-end encryption, etc.

Considering the transportation network is part of the critical infrastructure, security requirements for its information systems are typically higher. This is due to the significance of the potential impact of a cyberattack on the economy, service provision, as well as public safety. This underlines the importance of applying the European Common Criteria-based Cybersecurity Certification Scheme (EUCC) 2024/482. The scheme aims to set the framework for certifying ICT products to ensure they meet the standard requirements for cybersecurity. In the EUCC, certification bodies can issue EUCC certificates at two assurance levels: "Substantial" and "High". According to EU Cybersecurity Act Regulation 2019/881, which is the primary legislation to the EUCC 2024/482, a "Substantial" assurance level ensures that the ICT products, services, and processes meet security requirements and are evaluated to minimise known cybersecurity risks from attackers with limited skills and resources. At the "High" assurance level, the certificate ensures that the ICT systems adhere to more advanced security standards, designed for resistance to attacks from skilled attackers. Each assurance level



corresponds to a specific vulnerability assessment family under the Common Criteria, also known as AVA\_VAN. The AVA\_VAN level refers to the assurance vulnerability analysis level, indicating the extent of cybersecurity evaluation performed to assess the system's resistance to potential exploitation, weaknesses, or attacks in its operational environment, as defined by the common criteria standard. Cybersecurity certification can increase trust by ensuring that the data is secure from a potential cyberattack and, in the end, minimising the impact that could arise from them.

### 5.3.1.1. Organisational Approach for Ensuring Suitable Trust Mechanism

The organisational approach for ensuring trust within the TN-ITS data chain requires a certain degree of cooperation between the data provider and the service provider. The approach is inspired by TM2.0, an ERTICO innovation platform, and is based on the principles of collaboration and trust, alignment of information to drivers and consistency, co-opetition, understanding among stakeholders on interests and needs, and integrated information and control loops.

TM2.0 produces 'levels of cooperation' between public and private partners and TN-ITS is using such a model, as the level of (human) cooperation is always the basis of the level of trust. Data exchange and usage resulting from intense cooperation between the service provider and the authority can be considered more trustworthy.

NAPCORE deliverable M4.2.6 mentioned this possibility in its research. This M4.2.7 document intends to further develop this model by defining the necessary minimum Service Level Agreement (SLA), Applicable licenses, and necessary minimum digital contract elements between the local/road authority and the service providers that define the level of cooperation and by consequence the levels of data trust.

The purpose of this agreement is to formally outline the collaborative efforts between various parties involved in the exchange of TN-ITS data. Firstly, it explicitly identifies all parties, including data providers, data recipients, and any third parties, along with their respective contact information. Secondly, it clearly defines the roles and responsibilities of each party within the data sharing ecosystem. These roles may encompass data ownership, data processing, or data control, with specific responsibilities assigned to each entity. Furthermore, the agreement adheres to the guidelines outlined in the RTTI Delegated Regulation 2022-670. The Road Authority acknowledges the dual role of both data owner and data retriever. While acting as a data owner, the Road Authority ensures that any data retrieved from external entities is governed by robust digital contracts, adhering to or exceeding the standards applied to contracts with service providers. Moreover, the Road Authority fulfils its role as a data processor as defined by the DR. Conversely, the digital map service provider assumes the role of a service provider as outlined within the framework of the DR. This structured approach fosters clarity, accountability, and compliance within the TN-ITS data chain framework.

### 5.3.2. Levels of Cooperation

In the context of TN-ITS mobility data sharing, cooperation between the data sender (the road authority) and the data receiver (digital map service providers) can be characterized at various



levels. These levels represent the extent and nature of cooperation, data sharing, and collaboration between the involved parties.

To simplify the levels of cooperation and align the implementation and enforcement strategies accordingly, three broader cooperation categories have been identified, with No Cooperation totalling four levels. It should be noted that these categories are based on the six levels of cooperation as proposed by the TM2.0 initiative. Each category will have tailored agreement content to match the complexity and depth of interaction required.

- **No Cooperation:** This level represents the case where there is no interaction between the road authority and a service provider and there are no legal obligations or mutual agreements.
- **Basic Cooperation (Combining No Cooperation, Minimal Cooperation):** This level includes scenarios where there is minimal to no direct data sharing or where data is shared openly with the public. Interactions are straightforward, with a focus on minimal restrictions, basic compliance, and transparency.
- **Intermediate Cooperation (Combining Partial Cooperation and Moderate Cooperation):** This level represents a moderate degree of data sharing and interaction, often driven by specific purposes or projects. There is a need for mutual agreements, moderate integration, and higher standards of security and governance.
- **Advanced Cooperation (Combining High Cooperation, Full Cooperation, and elements of Moderate Cooperation):** This level involves strategic partnerships or integrated ecosystems with extensive data sharing. It requires comprehensive legal agreements, high levels of integration, ongoing collaboration, and stringent security measures.

### 5.3.3. Key Considerations for Cooperation Levels

The level of cooperation between parties significantly impacts its success and effectiveness. Careful consideration of several key factors is crucial to establishing a collaborative framework that aligns with the specific needs and objectives of all stakeholders and is discussed below.

- **Data Privacy and Security:** Higher levels of cooperation require robust measures to ensure data privacy and security, especially when dealing with sensitive or personally identifiable information.
- **Legal and Regulatory Compliance:** Cooperation must align with data protection laws, EU data regulations, (EU Data Act), and contractual agreements.
- **Technical Compatibility:** Effective data sharing depends on compatible data formats, protocols, and interoperability standards between different systems and platforms. Although TN-ITS is well specified the typical implementations can differ.
- **Data Quality and Integrity:** To ensure that shared data is useful and reliable, both parties must commit to maintaining high data quality and integrity. As a basis, the



proposed TISA 5-star rating could be used as a reference for indicating the data quality level as well as the quality frameworks proposed by the NAPCORE WG3.

### Cross linking Level of Cooperation and Key Considerations:

Applying the key considerations (Data Privacy and Security, Legal and Regulatory Compliance, Technical Compatibility, and Data Quality and Integrity) to the levels of cooperation between data senders and receivers for mobility data sharing helps to identify how each consideration plays out at different cooperation levels. Table 13 documents how these considerations relate to each level of cooperation:

		<u>Basic co-operation</u>	<u>Intermediate co-operation</u>		<u>Advanced Cooperation</u>	
Considerations	No Cooperation	Minimal Cooperation	Partial Cooperation	Moderate Cooperation	High Cooperation	Full Cooperation
<b>Data Privacy and Security</b>	Minimal concerns, no data sharing	Anonymization, Security during sharing/exchange	Anonymization, secure transmission, encryption	Robust measures, VPNs, encryption	Comprehensive governance, real-time monitoring	Highest standards, Robust encryption, real-time detection
<b>Legal and Regulatory Compliance</b>	No data sharing agreements needed	Agreements for usage, GDPR compliance	Bilateral agreements for usage, retention, compliance	Detailed contracts, regular reviews	Extensive agreements covering all aspects	Comprehensive continually updated framework (1)
<b>Technical Compatibility</b>	Not applicable	Limited to Map service provider understanding	TN-ITS data exchange per DR 2022-670	Moderate integration, APIs, or platforms	High integration, jointly developed mechanisms	Complete integration, real-time exchange
<b>Data Quality and Integrity</b>	Internally managed	Ensured by the road authority, limited SP insight	Shared responsibility, validation agreements	Collaborative management, shared responsibility	Ongoing collaboration, continuous improvement	Automated validation, real-time checks

(1): The cell stating “Comprehensive and continuously updated frameworks” in the context of legal and regulatory compliance under the “Full Cooperation (Integrated Data Ecosystem)” level refers to the need for a robust, all-encompassing legal and regulatory structure that is regularly reviewed and modified to stay up-to-date with evolving laws, regulations, and industry standards.

Table 13 - Cross-linking Level of Cooperation and Key Considerations

### 5.3.4. TN-ITS Levels of Trust

Based on the discussion in previous sections, the proposed trust levels as per the key considerations are documented below and summarized:



Level of Cooperation	<u>Basic co-operation</u>	<u>Intermediate co-operation</u>	<u>Advanced Cooperation</u>
Level of Trust	<u>Level 1</u>	<u>Level 2</u>	<u>Level 3</u>
Description	Trust the receiver, clear purpose communication	Mutual trust, regular audits, Continuous communication, joint governance	High trust, regular joint meetings, Full transparency, clear governance

Table 14 - Proposed levels of trust

- **Trust level 1: Basic Cooperation (basic data trust)**

Data Privacy and Security: The authority must ensure that any TN-ITS shared data is anonymized or aggregated to protect privacy. Security measures are essential to prevent unauthorized access during the sharing process with the digital map service provider.

Legal and Regulatory Compliance: Agreements or terms of use need to be defined, specifying how the data can be used, stored, and protected by the service provider. Compliance with data protection regulations (e.g., GDPR) is necessary.

Technical Compatibility: Limited compatibility requirements but at least according to the TN-ITS specifications as TN-ITS data formats and transfer methods must be understood by the map service provider

Data Quality and Integrity: The authority ensures that the shared data is accurate and relevant, but the service provider might have an opinion about the obtained data's quality. (e.g. Applying the proposed star rating for data quality: 1 star)

- **Trust level 2: Intermediate Cooperation (Purpose-Driven Sharing)**

Data Privacy and Security: Data sharing by the authority is more frequent, so robust privacy measures (like anonymization and pseudonymization) and security protocols (such as VPNs, and encryption) are critical.

Legal and Regulatory Compliance: Detailed data-sharing contracts, specifying the purpose, scope, duration, and compliance requirements. Regular reviews to ensure ongoing compliance with regulations (RTTI DR 2022-670 compliance).

Technical Compatibility: A moderate level of system integration is required. APIs or data exchange platforms might be used to facilitate data sharing.

Data Quality and Integrity: Data quality management is more collaborative, with shared responsibilities for data validation, cleaning, and consistency. Map service providers provide syntax analysis feedback to the authority (feedback loop). Data accuracy is critical for achieving shared objectives. e.g. Applying the proposed star rating for data quality: 3 stars.

- **Trust level 3: Advanced Cooperation (Integrated Data Ecosystem)**

Data Privacy and Security: This level requires the highest standards of data privacy and security. Data must be continuously protected with robust encryption, identity management, and real-time threat detection. (Common Criteria level x certified systems at both the authority and the service provider)

**Legal and Regulatory Compliance:** Full cooperation necessitates comprehensive legal frameworks and compliance measures that are continuously updated to reflect evolving laws and regulations.

**Technical Compatibility:** Complete TN-ITS system integration. Close to real-time data exchange is required, interoperable systems, and advanced data infrastructure.

**Data Quality and Integrity:** Data quality is maintained through automated validation processes, real-time data quality checks, and robust data governance frameworks. Service providers provide both syntax and semantic feedback to the authority (Feedback loop) e.g. Applying the proposed star rating for data quality: 4 stars)

### 5.3.5. Approach for Ensuring Trust

The TN-ITS workshop on Trust and expert discussion sessions cumulated in an effective approach to establishing trust within the TN-ITS domain using a combination of tools. It is through the use of digital contracts between TN-ITS stakeholders, supported by Service Level Agreements (SLAs) for data quality, security, and trust, and signed using digital signatures. This approach ensures that organizations involved across TN-ITS data chain processes adhere to mutually agreed-upon standards, making their data transactions transparent, auditable, and enforceable. This section summarizes the tools table below with a detailed description documented in the subsequent chapter.

**Note:** A sample TN-ITS Trust Digital Contract is presented in Annex D.

Component	Description	Role in the Proposed Trust Framework	Relation to Other Components
<b>Digital Contract</b>	A legally binding agreement defining the terms, conditions, and obligations of all parties.	Serves as the overarching framework that governs the relationship and specifies the inclusion of SLAs and digital signatures.	<ul style="list-style-type: none"> <li>- Specifies that SLAs are part of the contract.</li> <li>- Defines the use of digital signatures for authenticity and non-repudiation.</li> </ul>
<b>Service Level Agreement (SLA)</b>	A detailed appendix or section of the contract specifying performance metrics, service quality, and penalties.	Ensures measurable service standards and accountability for all parties involved.	<ul style="list-style-type: none"> <li>- Subordinate to the digital contract but directly referenced within it.</li> <li>- Often requires a digital signature to validate the agreement on specified SLAs.</li> </ul>
<b>Data License</b>	A legal instrument that grants permission to access, use, and share data under specific conditions.	Defines the scope, permissions, and restrictions for using shared data.	<ul style="list-style-type: none"> <li>- Integrated into the digital contract to specify rights and obligations related to data usage.</li> <li>- May include conditions tied to SLA performance requirements.</li> </ul>
<b>Digital Signature</b>	A cryptographic mechanism is used to authenticate and	Provides legal validity, integrity, and non-repudiation for the digital contract and associated SLAs.	<ul style="list-style-type: none"> <li>- Used to execute the digital contract and confirm agreement to the SLA terms.</li> <li>- Can be used for</li> </ul>

	verify the identity of signatories.		subsequent updates or amendments to the contract or SLA.
--	-------------------------------------	--	--

Table 15 – Tools to ensure organisational trust

- **Digital Contract**

Digital contracts are legally binding agreements between organizations that define the terms and conditions for data sharing, including responsibilities, expectations, and penalties for non-compliance. In the context of TN-ITS, these contracts ensure that all parties involved in the data chain (e.g., road authorities, map providers, and ITS service providers) adhere to agreed-upon standards for data quality, security, and trust.

- **Service Level Agreement**

Service Level Agreements (SLAs) are critical components of digital contracts, providing measurable benchmarks for trust in the data chain. For TN-ITS, SLAs can focus on specific data categories and respective quality criteria as well as security considerations, as documented in the table below for the three levels of trust.

SLA considerations	Trust Level 1	Trust Level 2	Trust Level 3
<b>Data use and purpose</b>	A clear definition of why the service provider uses TN-ITS	Detailed purpose and scope/use cases described	Detailed purpose and scope/use cases described
<b>Data quality</b>		3-star rating	<b>5-star rating</b>
<b>Data handling protection</b>	Guidelines	Security protocols defined	Automated and monitored
<b>Attribution requirements</b>	How is the authority credited?	How is the authority credited?	Collaborative Data Governance
<b>Compliance and legal requirements</b>	Adherence to regulations such as the GDPR	Regular review	
<b>Performance metrics Data access and transfer</b>	Adherence to TN-ITS standard	Data availability, response times, and reliability.	Include penalties for non-compliance

Table 16 – Proposed SLA considerations

- **Data License**

Selecting the appropriate license for data sharing depends on the level of cooperation and the specific goals, requirements, and concerns of the authority and the map service provider involved. The table below summarises the license recommendation for each level of cooperation.

	Trust Level 1	Trust Level 2	Trust Level 3
Proposed License	CC BY 4.0 (Creative Commons Attribution 4.0)	ODbL or Custom Data Sharing Agreement	Custom Data Sharing Framework or NLOD (Norwegian License for Open Government Data)
Description	This license allows the data authority to share data while retaining credit for their work. It requires attribution, ensuring that the map service provider acknowledges the source. This is suitable for minimal sharing where the authority wants to allow use but maintain recognition.	At this level, a license like ODbL can ensure that data is shared openly, and that derivative works maintain the same openness. However, due to the specific purposes and moderate integration involved, a custom data-sharing agreement is preferred to specify precise terms, including purpose, scope, and usage limitations tailored to the cooperation.	Full cooperation implies complete integration and shared governance. A custom framework that continuously adapts to legal and technological changes is essential. NLOD could be considered since TN-ITS data is from Member state road authorities and openness and accessibility are priorities. A custom framework should include comprehensive terms covering all aspects of the integrated data ecosystem.

Table 17 – Proposed License considerations

- **Digital Signature**

Digital signatures play a crucial role in establishing trust in digital contracts by ensuring authenticity, integrity, and non-repudiation. They work by using a public-private key pair, where the contract is signed with the stakeholder's private key, creating a unique digital signature that can be verified using the corresponding public key. This process confirms the identity of the signing parties, guarantees that the contract has not been altered after signing, and prevents any party from denying their involvement or commitments. Tools like Adobe Sign, DocuSign, or EU-compliant eIDAS-based solutions can be used to implement digital signatures, ensuring compliance with EU regulations while providing a secure and efficient way to formalize agreements in the TN-ITS data chain.

### 5.3.6. Trust Recommendations

Several industries have already implemented digital contracts with service-level agreements (SLAs) and digital signatures to ensure data trust. A very relevant example is the EU Mobility Data Space (MDS), where transportation organizations, service providers, and government agencies exchange mobility-related data under well-defined SLAs. These agreements specify parameters such as data accuracy, update frequency, and access permissions, ensuring that all participants adhere to a shared standard. By signing these contracts using eIDAS-qualified digital signatures, organizations establish a legally binding and tamper-proof foundation for trust. This approach not only safeguards the integrity and security of mobility data but also facilitates interoperability between different transport networks, allowing for seamless, real-time data exchanges.

## 5.4. TN-ITS quality

Data quality within the TN-ITS ecosystem is a critical component for the effective and safe operation of Intelligent Transport Systems (ITS) across Europe. Given the complexity of TN-ITS, which crosses a vast network of stakeholders, data sources, and applications, it is essential to develop a robust, scalable, and context-sensitive quality approach. TN-ITS data quality has a highlighted importance according to the European ITS Platform (EU-EIP). EU-EIP is functioning as a technical knowledge management centre for ITS deployment in the EU<sup>56</sup>. Efficiency and acceptance of ITS services are the functions of the quality targets from the perspective of the traveller. Therefore, there is a clear need for a widely known and widely accepted approach to defining quality aspects and related quality levels for TN-ITS data.

### 5.4.1. Approach for ensuring suitable data quality mechanism

In this chapter, we propose an optimized quality approach that integrates best practices from the TN-ITS GO and EU-EIP frameworks, previously presented and developed in Milestone 4.2.6, as well as new approaches introduced in this report, such as the TISA 5-Star Rating System and the Quality Frameworks (QFs) from the NAPCORE project, as detailed in Section 2.2, where they were discussed alongside other relevant projects and initiatives. Therefore, a detailed explanation of these frameworks will not be repeated in this chapter. The focus will be on the practical application and optimization of the quality approach for TN-ITS.

The approach for ensuring a suitable data quality mechanism will be explained next, including suggestions for optimal quality criteria, quality levels, the minimum required level, and continuous monitoring methods.

### 5.4.2. Definition of Quality Criteria

A fundamental aspect of the proposed approach is the clear definition of quality criteria. These criteria must be measurable and applicable across different stages of the TN-ITS data chain, from data collection to data usage. Below are the basic quality criteria that serve as a foundation for assessing data quality within quality within TN-ITS and whenever possible, they are presented using the speed limit use case:

- **Accuracy:** This criterion refers to the extent to which the data accurately represents real-world conditions. A key component of accuracy is location accuracy, which is critical for applications like navigation and automated driving. The accuracy of static speed limit data, for example, must be precise to ensure correct implementation in systems that depend on geospatial information.
- **Geographic Coverage:** This criterion assesses the extent to which data covers the required geographic area. Comprehensive geographic coverage ensures that all relevant locations are included in the dataset, which is particularly important for applications like national traffic management systems where gaps in coverage could lead to incomplete or misleading information.

<sup>56</sup> EUEIP European ITS Platform, *Online Workshop on Truck Parking Information Quality*, December 2020, [https://www.its-platform.eu/wp-content/uploads/TIS-Platform/AchievementsDocuments/QualityFrameworks/EU\\_EIP\\_4.1-201217\\_Truck\\_Parking\\_Quality\\_Workshop\\_Slides.pdf](https://www.its-platform.eu/wp-content/uploads/TIS-Platform/AchievementsDocuments/QualityFrameworks/EU_EIP_4.1-201217_Truck_Parking_Quality_Workshop_Slides.pdf)



- **Timeliness:** This criterion measures the speed at which data is updated and made available. Timeliness is crucial for real-time applications such as traffic management and incident response, where outdated information can lead to ineffective or even harmful decisions. It also includes the concept of pre-announcement of changes, which ensures that critical updates are communicated ahead of time. However, considering that this report is based on TN-ITS data-chain (static data) it is imperative to mention that, for TN-ITS, this criterion has a different approach. According to the TN-ITS Go project, Timeliness is the time from initial regulation to the publication of the related digital dataset.
- **Latency:** This criterion refers to the delay between data generation and its availability for use. Lower latency is particularly important for real-time decision-making processes in dynamic environments, such as managing traffic flow or responding to incidents. It directly impacts the effectiveness of systems that rely on the immediate availability of fresh data.
- **Completeness:** Refers to the extent to which all necessary speed limit data is included in the dataset. This includes ensuring that every relevant road segment has an associated speed limit value and that no segments are left without data coverage. Missing speed limit data can result in incorrect or unsafe driving recommendations, especially in systems that rely on comprehensive information for navigation and automated driving.
- **Consistency:** The degree to which data is uniform across different sources and stages of processing, essential for ensuring that data can be reliably integrated and used across various platforms. In the context of speed limits, consistency ensures that the speed limit information remains the same across various systems (e.g., mapping applications, navigation systems, and regulatory databases) and that there are no discrepancies in the data presented to users. Consistent data is crucial for ensuring that drivers receive the same speed limit information regardless of the platform they are using.
- **Correctness:** This criterion overall rightness or validity of the data in the context of the system's rules and expectations. For speed limits, correctness would mean that the speed limits are not only accurate but also correctly classified, represented, and consistently applied across the dataset. It also encompasses ensuring that the speed limits are correctly categorized and fit the expected patterns or regulations.
- **Error Rate:** Error rate refers to the frequency of errors within the speed limit data, such as incorrect speed limit values or misaligned geographic references. A low error rate is critical for maintaining high data quality, as errors in speed limit information can lead to unsafe driving behaviour, non-compliance with traffic laws, and reduced trust in navigation systems.

While these criteria provide a solid foundation, it is also crucial to understand how these elements are reflected in the different quality frameworks applied within the TN-ITS ecosystem. The table below provides a detailed comparison of the key quality criteria across the TN-ITS GO, EU-EIP, and the TISA 5-Star Rating frameworks, specifically for the speed limits use case.

**Note 1:** The Quality Frameworks from the NAPCORE project have not been considered in this analysis because the final reports (milestone) for each quality framework, including the



complete list of quality criteria, have not yet been completed. Furthermore, although TISA also released the TISA ISA framework for Digital Maps, it has not been included in this table. After review, the definitions used for the TISA 5-Star Rating framework was found to be similar and did not warrant a need to be added at this stage.

**Note 2:** Not all quality criteria listed in the table are directly related to the "Speed Limit" use case. These criteria are included for broader context and future reference.

**Note 3:** The following table does not represent all the quality criteria presented by each of the three frameworks.

Quality Criteria	EU-EIP (SRTI & RTTI)	TN-ITS Go	TISA 5-Star Rating (Static Speed Limit)
<b>Accuracy</b>	<b>Location accuracy:</b> The relative accuracy of the referenced location for the speed limit concerning the actual location of the event.	<b>Accuracy:</b> Geolocation is crucial for ensuring that speed limit data is accurate and up-to-date.	<b>Accuracy:</b> Precision in meters depending on the star rating, ensuring accurate representation of speed limits in specific locations. Related to accuracy, there are also other criteria such as Location Referencing (coordinates), Linear Referencing, and Direction Defined.
<b>Geographic Coverage</b>	<b>Geographical Coverage:</b> The percentage of the road network covered by the content provision service, ensuring comprehensive inclusion of all relevant road segments.	<b>Geo coverage representation:</b> The scope of geographic coverage in TN-ITS Go is intended to cover 7% of the network, with a revision of the RTTI delegated act focusing on primary roads.	-
<b>Timeliness</b>	<b>Timeliness (start and update):</b> The time between the occurrence of an event and the acceptance of the event, as well as how quickly updates are reflected.	<b>Timeliness:</b> The procedure aims to improve the throughput time from initial regulation to the publication of the related digital dataset. Metadata description and last change timestamp are provided for operational excellence.	<b>Timeliness:</b> Degree to how quickly data or information is collected, processed, and made available and accessible in a database.
<b>Latency</b>	<b>Latency (content side):</b> The time between the acceptance of an event or its end or (safety) relevant change of condition and the moment the information is provided by the content access point.	<b>Latency:</b> Ensures minimal delay between the time data is generated and when it is available for use. Emphasizes the importance of freshness and operational efficiency.	<b>Update Cycle:</b> This is the process of periodically refreshing, modifying, and publishing data so that it is accessible by 3rd parties.

<b>Completeness</b>	<b>Event coverage:</b> The percentage of events that are correctly detected and published, by type/class, time, and location.	<b>Completeness:</b> Involves the thoroughness of the dataset in covering all necessary speed limit data. TN-ITS Go ensures that data includes all relevant segments to prevent navigation or safety issues.	<b>Completeness:</b> Coverage of speed limits across all necessary routes and classifications, from >80% to >99%, depending on the star rating.
<b>Consistency</b>	-	<b>Consistency, coherence, or clarity:</b> TN-ITS Go focuses on ensuring that the speed limit data is consistent, coherent, and clear across different stages of processing.	-
<b>Correctness</b>	<b>Classification Correctness:</b> The accuracy and appropriateness of speed limit classifications within the dataset, ensuring alignment with regulatory and system rules.	<b>Correctness:</b> The correctness of speed limit data in TN-ITS Go is monitored through feedback loops to ensure alignment with regulatory standards.	<b>Correctness:</b> Ensures speed limits are accurately represented and correctly classified, with correctness levels ranging from >80% to >99% depending on the star rating.
<b>Error Rate</b>	<b>Error Rate:</b> The percentage of published status reports showing excessive deviations of a reported quantity (e.g., speed or travel time) versus the actual value or are otherwise determined as erroneous.	(Implicit in correctness criterion data inherently includes minimizing errors, with a focus on reducing inaccuracies through validation tools like HERE and TomTom.)	(Implicit in correctness criterion, with specific targets set to ensure the reliability and safety of the speed limit information provided.)

Table 18 - Quality Criteria Across the Different Frameworks<sup>57</sup>

This comparative approach provides a comprehensive understanding of how each framework addresses specific data quality, helping stakeholders choose the most appropriate criteria and framework for their specific needs.

### 5.4.3. Levels of Quality

Given the existing frameworks, each initiative suggests different levels of quality according to their needs. Below is a comparison table that outlines the quality levels defined within the TISA, EU-EIP, and TN-ITS GO frameworks:

Framework	Level 1	Level 2	Level 3	Level 4	Level 5
-----------	---------	---------	---------	---------	---------

<sup>57</sup> See, Source of data: 1 – TN-ITS GO, *D2.3 Data Store maintenance and TN-ITS service roll-out (consolidated)*, January 2024, [D-2.3-Data-store-maintanance-and-TN-ITS-service-roll-out.pdf](#), 2 – EUEIP European ITS Platform, *Working on common Frameworks for the Quality of European ITS Services and their Data*, 2020, [Working on common Frameworks for the Quality of European ITS Services and their Data - European ITS Platform \(its-platform.eu\)](#), 3 -TISA, *EU RTTI 5-Star Rating*, March 2024 [PowerPoint Presentation \(tisa.org\)](#)



<b>TISA 5-Star Rating</b>	<b>Star 1 &amp; 2:</b> If the data is below the agreed minimum quality standard, there is no guarantee the data will be used by ITS Service Providers.		<b>Star 3, 4 &amp; 5:</b> If the data meets the commonly agreed minimum quality standard or higher, ITS Service Providers will use the data.		
<b>EU-EIP</b>	<b>Basic:</b> Meets regulatory requirements and provides basic functionality	<b>Enhanced:</b> Significant improvement in data quality, suitable for more demanding applications	<b>Advanced:</b> Highest data quality, required for critical applications	N/A	N/A
<b>TN-ITS GO</b>	<b>Basic (Low):</b> Meets essential regulatory requirements	<b>Elite (Medium):</b> Improved accuracy, consistency, and reliability	<b>Ultimate (High):</b> High precision and reliability for critical applications	N/A	N/A

Table 19 - Quality Levels in each different Framework

The ISA framework for Digital Maps recently in November 2024 released from TISA presents a different method for testing quality levels, by focusing on performance testing in different operational and technical environments, allowing map providers to conduct their quality assessment and benchmarking more suitable for their own needs.

This framework was released at the ending stages of this milestone’s development and as a result, it was not possible to do a deeper analysis of it at this stage. A recommendation for future investigation could be outlined in actions such as NAPCORE-X (the successor of NAPCORE project), where this framework might be considered for a more in-depth study. However, it is worth noting some differences that were observed between the levels of quality approach and the testing environments suggested by the ISA framework.

**Differences between Levels of Quality approach vs testing environments:**

The TISA ISA framework for Digital Maps takes a different approach compared to the levels of quality approach suggested in the table above. While the 5-Star Rating framework evaluates the performance of Real-Time Traffic Information (RTTI) services based on external and user-facing criteria, the ISA framework focuses on internal processes that cater specifically to map providers' operational needs. The ISA framework emphasizes enabling map providers to conduct detailed tests on their data. This approach allows potential issues to be identified and resolved early in the process, serving as a complementary measure to the 5-Star Rating framework. By performing in-house quality checks first, map providers can ensure their data meets necessary standards before it undergoes external evaluation or is integrated into broader RTTI systems.

Additionally, the ISA framework’s focus on internal testing and validation provides a structured approach for ensuring accuracy and consistency. This allows map providers to refine their data within controlled conditions, reducing errors and improving the overall



quality of the maps. The combination of internal assessments and external evaluations creates a more thorough process for delivering reliable and high-quality digital maps suitable for a wide range of applications.

#### 5.4.4. TN-ITS data chain quality levels analysis

Within this task group, as well as among the broader ITS community, there has been an ongoing discussion regarding the adoption of three or five quality levels. This report does not aim to take a definitive stance on either option but rather seeks to present the potential advantages and disadvantages of each approach, fostering an informed and evidence-based analysis by the stakeholders. This section examines the benefits and challenges associated with implementing either three or five quality levels for data management, focusing on factors such as simplicity versus precision, flexibility, and alignment with established regulatory frameworks.

#### Advantages and Disadvantages of Three vs. Five Quality Levels:

- Three Quality Levels
  - a) Advantages
    - **Simplicity:** Easier for stakeholders to understand and implement, reducing complexity in data management.
    - **Clarity:** Clear distinctions between levels can help avoid ambiguity in quality assessments.
    - **Alignment with Existing Frameworks:** Consistent with the TN-ITS GO and EU-EIP frameworks, facilitating integration and comparison.
  - b) Disadvantages
    - **Lack of Granularity:** This may not capture subtle differences in data quality needed for certain advanced applications.
    - **Limited Flexibility:** Fewer levels may restrict the ability to tailor quality assessments to specific use cases.
  
- Five Quality Levels
  - a) Advantages
    - **Greater Precision:** Allows for more nuanced assessments of data quality, particularly useful in complex or high-risk environments.
    - **Enhanced Flexibility:** Provides more options for stakeholders to choose the most appropriate quality level for their needs.
  - b) Disadvantages
    - **Increased Complexity:** More levels can lead to confusion or difficulties in implementation, particularly for less sophisticated stakeholders.
    - **Potential for Overlap:** The distinctions between levels may become less clear, leading to ambiguity in assessments.

### 5.4.5. Minimum Level Requirement

Determining the minimum level of data quality required for different applications remains a topic of ongoing discussion. Within the RTTI Task Force<sup>58</sup>, which is part of the NAPCORE project, active efforts are underway to develop a potential approach in this regard.

To provide a more comprehensive analysis for the readers, all the information provided in table 19 was considered and, initiatives and projects were chosen as examples in relation with level 2 and level 3. While this work is ongoing, we offer the following preliminary essential theme suggestions for a three-level quality approach:

- **Level 1 - General Traffic Information:** Level 1 might suffice, providing a basic level of accuracy and timeliness needed for most non-critical applications. A navigation system using Level 1 data might be adequate for most users but may struggle with precision in dense urban areas where exact location data is critical.
- **Level 2 - Advanced Driver Assistance Systems (ADAS):** Level 2 should be the minimum requirement, ensuring greater accuracy and consistency for semi-automated driving features. A traffic management system using Level 2 data can optimize vehicle flow in real-time, enhancing efficiency and reducing congestion.
- **Level 3 - Fully Automated Driving:** Level 3 should be the baseline, guaranteeing the highest level of reliability necessary for safe operation. Autonomous vehicles in urban environments require Level 3 data to ensure accurate real-time decision-making and safety.

These suggestions are provisional and should be refined in collaboration with ongoing efforts within the NAPCORE RTTI Task Force.

### 5.4.6. Monitoring Quality and Evaluation Methods

To maintain data quality over time, continuous monitoring and evaluation mechanisms should be implemented. General methods for preserving the quality of data, as specified within the NAPCORE project's grant agreement, include:

- **Continuous monitoring of equipment performance and availability:** Ensuring that the data collection and transmission equipment is functioning correctly and consistently.
- **Manual verification of entities, events, or conditions:** Conducting spot checks and manual reviews to ensure data accuracy and reliability.
- **Monitoring of data completeness and latency:** Regularly checking that data sets are complete and that the time between data generation and availability is minimized.
- **Monitoring of timeliness:** Ensuring that data is updated and comprehensive enough to meet the needs of the applications.
- **Surveys of perceived quality by users:** Gathering feedback from end-users on the perceived quality of the data.
- **Collection of direct user feedback:** Actively seeking input from users to identify any issues with data quality.

<sup>58</sup> NAPCORE, *Working together on the implementation of the revised RTTI Delegated Regulation*, November 2023, <https://www.napcore.eu/documents/proceedings2023/RTTI.pdf>



- **Monitoring of service by using statistics:** Utilizing statistical analysis to track the performance and quality of data services.
- **Automated anomaly detection:** Implementing machine learning algorithms to detect and flag anomalies in data that may indicate quality issues.
- **Data validation rules:** Setting up automated checks that enforce specific rules for data input, ensuring that data meets predefined quality standards.
- **Cross-referencing with external data sources:** Comparing TN-ITS data with other reliable data sources to identify and correct discrepancies.
- **Regular audits and reviews:** Conducting scheduled audits and comprehensive reviews to ensure that quality control measures are effective and up-to-date.

These methods, combined with the continuous improvement cycle, ensure that the TN-ITS data remains reliable, accurate, and fit for purpose across all applications.

#### 5.4.7. Quality Recommendations

In conclusion, the TN-ITS quality framework presented in this chapter aims to establish a robust and scalable approach to ensuring high standards of data quality across the TN-ITS ecosystem. By integrating well-established frameworks such as TN-ITS GO and EU-EIP with newer approaches like the TISA 5-Star Rating and the TISA Guideline for Digital Maps and drawing insights from the ongoing NAPCORE project, the proposed model is designed to meet the diverse needs of stakeholders involved in ITS.

#### Recommendations for the TN-ITS community:

1. **Adopt the TISA Quality Criteria:** Given that the TISA 5-Star Rating approach is regularly updated and aligned with the latest developments in ITS, it is recommended that the TISA quality criteria be considered as a reference for ensuring that data remains relevant and up-to-date.
2. **Follow the Three-Level Quality Model:** It is recommended that TN-ITS adopt the three-level quality model, as it provides a clear and straightforward framework that aligns well with TN-ITS GO and EU-EIP standards within the next 10 years. This approach balances simplicity with the need for effective data management across different use cases. While the list of criteria for the TISA 5-star rating is relevant, the three-level model appears to be sufficient to ensure the required quality.
3. **Set Minimum Required Level to Level 2:** For achieving excellence in data quality that meets the current realities and needs in the European Union, setting the minimum required quality level at Level 2 is considered sufficient within the next 10 years. This level ensures a high standard of data accuracy, timeliness, and reliability, which is adequate for most ITS applications today.
4. **Suggest map providers utilize the TISA ISA framework for Digital Maps:** To ensure that map providers add high quality data to the data chain, it is recommended that they utilize the testing environments suggested by the TISA ISA Guideline paper.
5. **Continuous Monitoring and Improvement:** Implementing the monitoring and evaluation mechanisms outlined in this chapter will be crucial for maintaining data quality over time. Regular audits, user feedback, and automated anomaly detection should be standard practices to ensure the reliability and accuracy of TN-ITS data.

6. **Alignment with Emerging Standards:** As the NAPCORE project finalizes its quality frameworks, it is advisable to revisit the TN-ITS quality approach to ensure alignment with these new standards. This will help ensure that TN-ITS data remains current and compliant with the latest European initiatives in ITS.
7. **Stakeholder Collaboration:** Successful implementation of the quality framework requires ongoing collaboration among all stakeholders, including regulators, technology developers, and end-users. Establishing working groups or discussion forums can facilitate this collaboration and help address challenges as they arise.
8. **Future Comparative Analysis of Quality Criteria Values:** In the future, it will be valuable to assess and compare the specific values associated with each quality criterion across the different frameworks. A detailed comparative analysis will provide deeper insights into the strengths and weaknesses of each approach. In the meantime, we recommend that the quality criteria values from the TISA 5-Star Rating be used as a benchmark.

By following these recommendations, the TN-ITS ecosystem can maintain its commitment to high data quality standards, ensuring the effective and safe operation of ITS across Europe.

## 5.5. TN-ITS sovereignty

Data sovereignty is a legal concept that encompasses the rights and controls an entity holds over its data, dictating access, management, and usage permissions. It refers to the ability of an entity to manage its data independently from others, ensuring that the data is subject to the laws and governance structures within the nation where it is collected, stored, or processed. This plays a crucial role in maintaining data quality, integrity, security, and trust among the Stakeholders within the TN-ITS ecosystem.

### 5.5.1. Approach for Ensuring a Suitable Data Sovereignty Mechanism

In this context, this document focuses on sovereignty to secure the quality of data in the Data Chain from collection to use. Data protection from a political perspective is not in the scope of this writing.

#### Legal Frameworks and Regulations

As a backbone for the interstate sharing of data, The European Data Act (applicable in 2025) defines essential requirements regarding interoperability to ensure that data can flow seamlessly between sectors and Member States as well as between data processing services providers in the Data Chain (Regulation (EU) 2023/2854)<sup>59</sup>.

The Data Act is instrumental in creating Common European Data Spaces. These EU-wide, interoperable data spaces in strategic sectors are designed to eliminate existing legal and technical barriers to data sharing, thereby unlocking significant potential for data-driven innovation. These common European data spaces are logically and coherently linked with

<sup>59</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_202302854&qid=1724321225518](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854&qid=1724321225518)



other regional, national, and transnational initiatives for data infrastructures, aiming to create a federated data infrastructure based on European values of data and cloud sovereignty.

### **Common European Data Spaces**

Common European Data Spaces bring together relevant data infrastructures and governance frameworks to facilitate efficient data pooling and sharing. They include data governance structures that comply with EU legislation, transparently and fairly defining rights related to data access and processing. This approach enhances the availability, quality, and interoperability of data, ensuring that data from across the EU can be made available and exchanged in a trustworthy and secure manner. Businesses, public administrations, and individuals in Europe will have control over the data they generate, with the confidence that it is managed and used securely and responsibly<sup>60</sup>.

### **Data Ownership and Control**

Data sovereignty also involves managing data ownership and control. Original data ownership includes legal rights to create, edit, modify, share, and control data access. Challenges arise with enriched data—data that has been modified or enhanced by another stakeholder—which may create grey areas in ownership. Organizations can manage their data ownership rights effectively through strategies such as robust data protection and control, clear data access rights, transparency, and adherence to the FAIR Data Principles.

### **Security and Compliance**

Adherence to security standards, such as encryption and access controls, is essential for maintaining data integrity and sovereignty. Localized data storage and processing ensure that data complies with the legal requirements of the Member State's jurisdiction and EU regulations. This localized approach makes it easier to monitor and maintain data quality, while compliance with non-legislative acts like the RTTI Directive and standards like TN-ITS and DATEX II further enhances trust and data security.

## **5.5.2. Implications of Data Sovereignty**

In summary, data sovereignty ensures that data is governed by local laws and regulations, which often include stringent data protection and privacy laws. This governance framework warrants that data security practices align with the specific legal requirements of the country, thereby reducing the risk of non-compliance and potential legal repercussions. By keeping data within national borders, organizations gain control over who can access the data and how it is used, minimizing the risks of unauthorized access and breaches. Localizing data helps in holding entities accountable under local laws for any breaches or mishandling of data. This promotes more responsible data management practices and encourages compliance with national standards. Moreover, countries may enforce specific standards on data centers and infrastructure within their borders, ensuring that both physical and cyber protections are robust and effective.

---

<sup>60</sup> European Commission, *Commission staff working document on Common European Data Spaces*, 2022, <https://ec.europa.eu/newsroom/dae/redirection/document/83562>



### Challenges of Data Sovereignty and Integrity in Multi-Jurisdictional Contexts:

Storing data within an overarching jurisdiction can limit exposure to international threats and legal conflicts that may arise from data being stored or processed across multiple countries with varying legal frameworks. This can lead to inconsistencies in how data is managed, shared, and protected, especially when the data crosses borders within the EU or beyond.

Regarding the RTTI Delegated Regulation, while it stipulates that data provided by the authority must be used by the service provider if available, the concern arises when service providers alter this data. This is a critical issue that warrants further discussion. Altering authoritative data could potentially compromise its integrity, leading to inconsistencies and reduced trust in the data being shared across the TN-ITS ecosystem. One possible approach to address this could be to establish clear guidelines or limitations on how data can be altered by service providers. These guidelines should ensure that any modifications do not undermine the original data's accuracy, reliability, or trustworthiness. Furthermore, there should be transparency in any alterations made, with clear documentation (through metadata for example) of changes to ensure traceability and accountability.

Furthermore, stakeholders maintain ownership over their published data, often referred to as original data ownership. This ownership includes a range of legal rights over data, such as the ability to create, edit, modify, share, and control access to the data. Additionally, stakeholders have the right to delegate, share, or transfer these rights to a third party. However, when another stakeholder enriches the data and republishes it for usage, the ownership of the enriched data can become a grey area. The resolution of such ownership issues may depend on the terms of the original data use agreement, the nature of the enrichment, and applicable laws and regulations.

Organizations can effectively manage their data ownership rights when sharing data with others by following these strategies:

- **Data Protection and Control:** Implement robust data management practices that comply with various regulations and secure sensitive information against unauthorized access and breaches.
- **Data Access Rights:** Clearly define the responsibilities of all parties involved in data sharing. This includes determining who has access to the data, how it is processed, and where it is stored<sup>61</sup>.
- **Transparency:** Communicate to individuals that their data may be shared and for what purpose, ensuring that they are informed and can provide informed consent.
- **Data Stewardship:** Implicit in the idea of ownership of data is the concept of stewardship of data, which includes the creation, access, modification, sale, storage, and the ability to assign or license any of these privileges to others.

<sup>61</sup> Thouvenin Florent & Aurelia Tamo-Larrieux, *Data Ownership and Data Access Rights*, July 2021, <https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-ownership-and-data-access-rights/BC314C63C58A09C4B9C5D55894FE68C6>



- **FAIR Data Principles:** For open data, adhere to the FAIR Data Principles to maximize the value of shared data by making it Findable, Accessible, Interoperable, and Reusable<sup>62</sup>.

---

<sup>62</sup> Wilkinson, M., Dumontier, M., Aalbersberg, I., et al, *The Fair Guiding Principles for scientific data management and stewardship*, 2016, <https://www.nature.com/articles/sdata201618#citeas>



## 6. Data chain evaluation tools and best practices for optimal TN-ITS system

This chapter covers the landscape of data chain evaluation tools and best practices within the TN-ITS framework, aiming to enhance the five critical data aspects discussed earlier. The focus is on recommending assessment methods and tools that ensure compliance with and adherence to high-quality TN-ITS standards. The chapter emphasizes the potential for validating these standards, offering stakeholders a structured approach to assess and enhance their data practices.

### 6.1. Requirements for data evaluation tools

In developing effective data evaluation tools within the TN-ITS framework, several considerations arise from the discussions on the TN-ITS data chain, documented in previous chapters. The enrichment and assessment tools suggested subsequently are classified by their significance and should correlate with roles (responsibilities), data chain stages, data aspects, and additional relevant criteria such as level of feasibility (at an organizational and legal level) and business prospect, ensuring robustness and practicality in their application.

### 6.2. Categories of Data Evaluation Tools

The assessment tools are categorized into well-defined groups to facilitate their classification and application. Organizing these tools into specific categories enhances clarity and accessibility, enabling stakeholders to effectively navigate and select tools that align with their objectives and requirements for improving TN-ITS trustworthiness among the stakeholders and improving data quality, trust, security, integrity, and sovereignty. The categories of tools are as follows:

- I. **Semantic Validation Tools:** Ensure that the data's meaning is correct and consistent with the intended context.
- II. **Syntactic Validation Tools:** Verify that the data structure and format adhere to predefined rules and standards.
- III. **Compliance Assessment:** Evaluate whether the data and processes meet regulatory and policy requirements.
- IV. **Security Audits:** Examine the data chain for vulnerabilities and ensure protection against unauthorized access.
- V. **Authentication, Authorisation & Accounting Services:** Manage user identities, permissions, track usage for security and accountability.
- VI. **Metadata:** Provide descriptive information about data to facilitate its understanding, use, and management.
- VII. **Feedback Loop:** Mechanism for data-chain actors to report issues and provide input to improve data quality and processes.
- VIII. **Service/Administrative Tools:** Tools for managing and supporting the operational aspects of the data chain.

### 6.3. Identification of data evaluation tools

This chapter lists the tools and methods relevant to improving the data aspects (quality, trust, security, integrity, and sovereignty) of the TN-ITS data chain, classified by the categories mentioned in the previous section as identified by the TN-ITS experts from the participating MS. These tools are deemed essential for ensuring that the exchange of information on changes in static road attributes is accurate and reliable.

For all the tools, an exhaustive analysis was conducted, associating each tool with the respective data aspects, responsible roles, and data stages of the TN-ITS data chain. While, in a broader sense, all stages, data aspects, and roles may have an indirect relationship with each tool, this milestone chose to focus on presenting only those with a more direct connection. This approach ensures clarity while acknowledging that multiple tools can still have indirect influences on other roles and data aspects across different stages of the data chain.

**Note:** Some of following tools, classified according to their high level of importance, will be explained in more detail later in this chapter. It is important to note that this milestone chose to focus on these tools as they were identified by the sub working group during their work as the most perceived important tools. After discussions and mutual agreements, they were shortlisted to be included as part of this deliverable.

The list of tools along with a brief description is presented as follows:

#### I. Semantic Validation Category:

- **Data type & enumeration checks** - Ensures that data types on the TN-ITS data are the expected ones and validates the correct use of enumeration values.

**Data aspects:** Quality | **Roles:** Data Holders and Data Users | **Data-Chain stages:** Data Collection and Data Processing

- **Version checks** - Verifies that the data schema version is up to date.

**Data aspects:** Quality | **Roles:** Data Users | **Data-Chain stages:** Data Processing

- **Data type & enumeration checks (Service)** – Validate data types and enumeration during the data retrieval from the Data Users.

**Data aspects:** Quality | **Roles:** Service Providers | **Data-Chain stages:** Data Exchange

- **Version check (Service)** – Conducts version checks during data retrieval from the Data Users.

**Data aspects:** Quality | **Roles:** Service Providers | **Data-Chain stages:** Data Exchange

- **Range checks** – Validate that data values fall within the allowable ranges (including compliance with the national laws).

**Data aspects:** Quality | **Roles:** Data Holders | **Data-Chain stages:** Data Collection

#### II. Syntactic Validation Category:

- **TN-ITS (XML) Validation Tool** - A tool developed during the TN-ITS Go to validate the schema based on the TN-ITS standard using Notepad++.

**Data aspects:** Quality | **Roles:** Data Users | **Data-Chain stages:** Data Processing



- **TN-ITS (XML) Validation Tool (FME)** - A tool developed during the TN-ITS Go to validate the schema based on the TN-ITS standard using the FME (Feature Manipulation Engine).

**Data aspects:** Quality | **Roles:** Data Users | **Data-Chain stages:** Data Processing

- **TN-ITS (XML) Validation Tool (Service)** - Service Providers conduct validation during the data retrieval from the Data Users.

**Data aspects:** Quality | **Roles:** Service Providers | **Data-Chain stages:** Data Exchange

### III. Compliance Assessment Category<sup>63</sup>:

- **Compliance Assessment tool - Declaration of Compliance** - Data users must submit a self-declaration of Compliance indicating that data registered on the NAP complies with relevant delegated regulation articles. The relevant articles of the DR must be considered during data collection. In addition, the assessment reports should include/monitor data timeliness, completeness, and latency.

**Data aspects:** Trust and Quality | **Roles:** Data Holders and Data Users | **Data-Chain stages:** Data Collection and Data Processing

### IV. Security Audits Category:

- **ISO 27001:2022 tool** - ISO 27001:2022 standard sets the governance aspects for the cybersecurity of an organization. It defines an Information Security Management System (ISMS) by defining the rules and the practices that can be implemented using the guidance of ISO 27002. The scope is defined on an organizational basis. ISO 27001 is the foundational standard for the C-ITS implementation and other national guidelines. Certificates are mutually recognized in Europe. ISO 27001 defines also internal audits. Security testing such as Penetration Testing on software and hardware is also provisioned by the application of ISO 27001. To attain the interoperability required by the NIS 2 directive (EU 2022/2555), the NAP security architecture should provide common guidance on a defined scope.

**Data aspects:** Security | **Roles:** Data Users | **Data-Chain stages:** Data Processing

- **Common Criteria (EUCS ISO 15408) tool** - The Common Criteria (CC) is a worldwide initiative aimed at defining a set of security profiles and criteria to test compliance to such profiles, that is performed in accredited laboratories. Recently, ENISA released the EU CC certification scheme, under the Cybersecurity Act (EU 2019/881) and further pushed by the proposed Cyber Resilience Act. It sets an EU marking for CE based on risk analysis. Typical implementations of the CC are C-ITS stations, firewalls, and operating systems. Certificates are mutually recognized under the SOG-IS agreement.

**Data aspects:** Security | **Roles:** Data Users and Service Providers | **Data-Chain stages:** Data Processing

### V. Authentication, Authorisation & Accounting Services Category:

- **Authorization ABB tool** - Provide network authorization for RESTful (REST: **RE**presentational **St**ate **T**ransfer) transactions, by using a standard mechanism (e.g., JWT token with a minimum format or SAML assertions). This is important as data should be disclosed and received only by authorized parties.

**Data aspects:** Security | **Roles:** Data Users and Service Providers | **Data-Chain stages:** Data Exchange

- **Node Authentication ABB tool** - Establishes secure communication channel using TLS (Transport Layer Security) 1.2 and 1.3, based on a consolidated and governed Public Key Infrastructure (PKI), to guarantee confidentiality and authentication of data in transit.

**Data aspects:** Security | **Roles:** All | **Data-Chain stages:** Data Exchange

- **Data Encryption ABB (XML-Enc as a possible extension) tool** – Ensures data confidentiality at rest, particularly in cloud services by using XML encryption for secure data storage. It's a security mechanism

<sup>63</sup> NAPCORE, *National Bodies*, last accessed January 2025, <https://napcore.eu/national-bodies-3/>



that assures the data confidentiality of transmitted messages. It's possible to encrypt an entire message or choose to encrypt only certain elements of the message. When a SOAP message is encrypted, only a service that knows the appropriate key can decrypt and read the message (<https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/>).

**Data aspects:** Security | **Roles:** Data Holders and Data Users | **Data-Chain stages:** Data Collection and Data Processing

- **Non-Repudiation ABB tool** – Provides non-repudiation services to generate, collect, maintain, make available, and validate the occurrence of an event. Usually, non-repudiation is used when a dispute arises (e.g., forensic analysis). There are several levels of non-repudiation. Typical basic non-repudiation is implemented by using digital signatures.

**Data aspects:** Security | **Roles:** Data Users | **Data-Chain stages:** Data Processing

- **Data Integrity ABB tool** - Data Integrity is defined as the act of guarding against improper information modification or destruction ensuring information non-repudiation and authenticity. Data Integrity defines integrity protection for data at rest. It fosters the usage of Enveloping, Enveloped, or Detached advanced electronic signatures. Data in transit is integrity-protected through XML Digital signatures or JSON signatures.

**Data aspects:** Integrity | **Roles:** All except End-Users | **Data-Chain stages:** Data Exchange

- **Data Provenance ABB tool** - Data Provenance is the foundation of data quality. In a decentralized or distributed setting where multiple sources share data with several endpoints, creating a chain of trust and quality among the stakeholders is crucial. Provenance has two different viewpoints: from the source, it answers the question “where the data goes”, while from the destination, answers the question “where the data comes from”. Moreover, Data Provenance tracks also all the permutations of data over its lifecycle.

**Data aspects:** Security and Integrity | **Roles:** All except End-Users | **Data-Chain stages:** Data Exchange

- **Access-Log: Web server generates access log tool** - Processes and analyses upload/POST action to provide insights into website or server activity. It can detect potentially malicious activity or security threats.

**Data aspects:** Security and Integrity | **Roles:** Data Holders, Data Users, and Service Providers | **Data-Chain stages:** Data Collection and Data Processing

- **Change-log tool** - Tracks modifications to files over time: version tracking, user attribution, timestamps, difference comparison, and conflict resolution.

**Data aspects:** Security and Integrity | **Roles:** Data Users | **Data-Chain stages:** Data Collection and Data Processing

- **Certified List tool** - Establishes a list of trusted entities or conditions that are allowed access. Restricts access to only those entities on the whitelist. Similar to the Credential List Manager from C-ITS DR.

**Data aspects:** Security and Integrity | **Roles:** Access Point and Service Providers | **Data-Chain stages:** Data Exchange

## VI. Standardized Metadata Schema Category:

- **mobilityDCAT-AP tool** - mobilityDCAT-AP<sup>64</sup> deployed by the sWG4.4 (NAPCORE) is an extension of DCAT-AP for describing mobility datasets, dataset series, and services. It provides an RDF syntax binding for the union of metadata elements defined in the National Access Points across Europe. The class Quality Annotation falls under the category of Optional classes, meaning it is not mandatory. This class is designed for free-text descriptions related to any quality aspects of the delivered content. In

<sup>64</sup> MobilityDCAT-AP Version 1.00 A mobility extension for the DCAT Application profile for data portals in Europe, October 2023, <https://mobilitydcat-ap.github.io/mobilityDCAT-AP/releases/1.0.0/index.html>



essence, it serves as an annotation encompassing methods, metrics/indicators, and results derived from a quality assessment. Similarly, certifications or digital contracts (such as for trust) can be represented by one of the free-text fields.

**Data aspects:** Quality and Trust | **Roles:** Data Holders and Data Users | **Data-Chain stages:** Data Collection and Data Processing

## VII. Feedback Loop Category:

- **Reporting tool** - Develop intuitive reporting tools for the end user and/or the service provider to report issues and provide feedback to the Service Providers and/or Data User/Data Holder (refer to the feedback scenarios).

**Data aspects:** All | **Roles:** Data Holders, Data Users, Service Providers, and End-Users | **Data-Chain:** Feedback Loop

- **Feedback Management tool** - Use (automated) systems to collect, process, and integrate feedback into decision-making workflows and dashboards. Respond accordingly to the feedback originator, hence completing the feedback loop.

**Data aspects:** All | **Roles:** Data Holders and Data Users | **Data-Chain:** Feedback Loop

- **Public Consultations tool** - Conduct periodic/regular public feedback sessions, such as seminars or targeted surveys to gain insight into the usage of data and identify gaps and need for new features/value-added services.

**Data aspects:** All | **Roles:** Service Providers and End-Users | **Data-Chain:** Feedback Loop

- **Assessment Incorporation tool** - Incorporate the findings/results from the compliance assessment process, such as self-declarations in the data chain.

**Data aspects:** All | **Roles:** Data Holders, Data Users, Access Point, and Service Providers | **Data-Chain:** Feedback Loop

- **Internal Feedback tool** - Specific Feedback concerning data, its quality, and format is exchanged between the Data Holder and Data User. The internal feedback can be implemented as a manual process such as a phone call/email or an automated process such as a customized API. The internal feedback can be extended to include the Access Point, based on the reality of each Member State.

**Data aspects:** All | **Roles:** Data Holders, Data Users, and Access Point | **Data-Chain:** Feedback Loop

## VIII. Service/Administrative Category:

- **SLA / Licenses tool** – Defines and verifies performance and availability standards for services such as software applications, network accessibility, and helpdesk support. They specify response times, resolution times, and uptime guarantees as well as associated licenses. An effective SLA typically includes Service Definition, Performance Metrics, Monitoring, Reporting, and Problem Management.

**Data aspects:** Trust and Sovereignty | **Roles:** Data Users, Access Point, and Service Providers | **Data-Chain:** All

- **Audits tool** – Performs automated audits to check if the service is following compliance guidelines and ensures data sovereignty by monitoring and enforcing local laws on data storage, processing, and transfer.

**Data aspects:** Quality and Sovereignty | **Roles:** Data Holders and Access Point | **Data-Chain:** Data Collection, Data Exchange and Feedback Loop

- **Digital Signature tool** – It's a security mechanism that provides authentication and integrity of metadata. It is used to ensure that the metadata has not been tampered with and that it comes from a trusted source.

**Data aspects:** Security and Integrity | **Roles:** Data Holders and Data Users | **Data-Chain:** Data Collection and Data Processing



● **Trust Certification tool** – Assigns trust certificates or digital contracts to/between the data holders and data users based on an agreed level of cooperation. If needed, the authenticity and integrity can be further ensured by digital signature.

**Data aspects:** Trust | **Roles:** Data Holders and Data Users | **Data-Chain:** Data Collection and Data Processing

#### 6.4. Data evaluation tools criteria

Following the process of selecting the most effective tools for enhancing the TN-ITS data chain, it is crucial to evaluate each tool against a set of predefined criteria. These criteria help ensure that the chosen tools not only address key data aspects such as quality, trust, security, integrity, and sovereignty but also align with organizational and legal requirements while offering significant business value for key stakeholders.

This section presents an in-depth analysis of each tool based on the following four criteria:

- a) **Level of Impact / Importance:** Assess the relevance and potential influence of each tool on critical data aspects.
- b) **Level of Implementation / Complexity:** Evaluate the technical challenges and resources required for implementing each tool.
- c) **Level of Organizational & Legal Complexity:** Examine the practical feasibility of implementation, considering both organizational and legal factors.
- d) **Business Prospect:** Analyse the potential return on investment or commercial relevance of each tool, whether immediate or mid-term.

To provide a comprehensive assessment that combines the performance of each tool across the four criteria while accounting for their differing importance, a **weighted average** was calculated. This method is advantageous as it enables the prioritisation of certain criteria over others, ensuring that the overall evaluation aligns with the relative significance of each criterion in the assessment process.

**Note:** For comprehensive details on the criteria and results of all data evaluation tools, please refer to Annex A.

Based on this analysis, the following sub-section provides a detailed exploration of the tools that received the highest scores in the "Level of Impact / Importance" criteria. The selected tools are analysed in greater detail to understand their specific contributions, implementation methodologies, and potential challenges.

##### 6.4.1. Level of impact/importance

The "Level of Impact / Importance" criterion assesses the relevance of each tool concerning critical data aspects such as quality, trust, security, integrity, and sovereignty. This criterion measures how much a tool can influence or improve these aspects within the context of the TN-ITS data chain.

The evaluation for this criterion follows a scale from 1 to 9, where:

- 1 - indicates that the tool has a very low impact/importance to the data aspects considered



- 3 - suggests a moderate impact
- 5 - reflects a significant impact
- 7 - represents high importance
- 9 - means the tool is of extreme importance and has a substantial impact on the data aspects

The top 5 most important tools after conducting this exercise are:

- Trust certification (stakeholders)
- Standardized metadata schema – DCAT-AP / mobilityDCAT-AP
- Feedback Loop tools
- Compliance assessment
- AAA Services - Authorization ABB; Node Authentication ABB

#### **6.4.2. Level of implementation complexity (technical)**

The "Level of Implementation / Complexity" criteria evaluate the technical difficulty involved in implementing each tool. This criterion is crucial for understanding the technical challenges and resources required to adopt each tool within the TN-ITS data chain.

The evaluation follows a scale from 1 to 9, where:

- 1 - indicates that the tool is easy to implement and requires few technical resources.
- 3 - suggests low complexity.
- 5 - reflects a moderate level of complexity.
- 7 - represents high complexity.
- 9 - indicates that the tool is extremely complex to implement, requiring advanced technical resources and considerable development time.

The top 5 most technically complex tools to implement:

- Trust Certification
- Compliance assessment
- Security Audits - Common Criteria (EUCC ISO 15408)
- Semantic Validation Tools – Range checks
- AAA Services - Data Encryption ABB; Data Provenance ABB; Certified List

#### **6.4.3. Level of organizational & legal complexity**

The "Level of Organizational & Legal" criterion examines the practical feasibility of implementing the tools, considering both organizational and legal aspects. This criterion evaluates the tool's alignment with existing policies, and regulations and the organization's ability to adopt and sustain the tool.

The evaluation uses a scale from 1 to 9, where:

- 1 - means the tool is easily feasible, both organizationally and legally.
- 3 - suggests moderate feasibility.
- 5 - reflects that the tool may face significant challenges but is still feasible.
- 7 - indicates that implementation may be difficult due to organizational or legal constraints.
- 9 - represents substantial barriers, making the tool difficult to implement under current conditions.



The top 5 tools most difficult to implement due to organizational or legal constraints:

- Security Audits - Common Criteria (EUCC ISO 15408)
- Trust Certification
- AAA Services - Data Provenance ABB; Certified List
- Compliance Assessment
- Digital Signature

#### 6.4.4. Level of business prospect

The "Business Prospect" criteria evaluate the potential return on investment or commercial relevance of each tool in terms of timeframe. This criterion measures whether the adoption of the tool will bring immediate benefits or is more aligned with mid-term objectives.

Tools are classified into two groups:

- Immediate Prospect: Tools that have an immediate commercial impact, offering quick returns or direct business benefits.
- Mid-term Prospect: Tools that, while important, are better suited for a mid-term strategy, with benefits that manifest over time.

The top 5 tools with the greatest business benefits and returns:

- AAA Services - Authorization ABB; Node Authentication ABB
- Feedback Loop tools - Internal feedback; Reporting tool
- SLA / Licenses
- Semantic Validation Tools - Data type & enumeration checks; Version check
- Syntactic Validation Tools - TN-ITS (XML) Validation Tool

#### 6.4.5. Weighted average of all criteria

In the intricate process of selecting the most effective tools for enhancing the TN-ITS data chain, it is crucial not only to evaluate each tool individually against predefined criteria but also to integrate these evaluations into a comprehensive, overall assessment. The application of a weighted average method facilitates this holistic approach, enabling the identification of tools that should be prioritized for immediate implementation.

Criteria weights justification:

- Level of Implementation Complexity (20%) - Lower complexity means faster deployment, making it important but less critical than impact or feasibility.
- Level of Impact/Importance (30%): This criterion has the highest weight because it directly measures the tool's potential to positively influence key data aspects, making it the most crucial factor in the decision process.
- Level of Organizational & Legal Complexity (25%): Feasibility is slightly less critical than impact but more important than technical complexity, as it ensures the tool can be effectively integrated within existing organizational and legal frameworks.

- Business Prospect (25%): Equal to feasibility, this weight highlights the importance of tools that offer immediate or near-term business benefits, balancing the practical and financial aspects of tool selection.

The weighted average is calculated using the following formula:

$$\text{Weighted Average (\%)} = \frac{(0.20 \times (10 - LC) + (0.30 \times LI) + (0.25 \times (10 - LL) + (0.25 \times IF(BP = \text{immediate}, 1, 0.5))))}{1}$$

Figure 12 - Weighted Average Formula of all criteria

Legend:

- **LC** - Level of Implementation Complexity (technical) – **20%** (converted as 10 minus LC to reflect that lower values are positive)
- **LI** - Level of Impact/Importance – **30%**
- **LL** - Level of Organizational/Legal Complexity – **25%** (converted as 10 minus LL to reflect that lower values are positive)
- **BP** - Business Prospect (immediate & mid-term) – **25%**
  - **Immediate** benefit (value 1)
  - **Mid-term** benefit (value 0.5)

Top 5 Tools (Weighted Average)

Based on the calculated weighted averages, the top 5 tools recommended for immediate implementation are (in percentage values):

- Semantic Validation Tools - Data type & enumeration checks (Service) – **84,29%**
- Semantic Validation Tools - Version check (Service) – **84,29%**
- Feedback Loop – Reporting tool – **81,43%**
- Semantic Validation Tools - Data type & enumeration checks – **78,57%**
- Semantic Validation Tools - Version check – **78,57%**

After analysing the complete list of tools, it is evident that the tools at the top of the list recommended for short-term implementation are those belonging to the categories of Semantic Validation Tools, Authentication, Authorization & Accounting Services, and Feedback Loop Tools.

## 6.5. Concepts and best practices for TN-ITS data evaluation tools

This section explores key concepts and best practices related to TN-ITS data evaluation tools. It highlights selected tools, from the previous list of tools (the criterion level of impact/importance), that play pivotal roles in enhancing the data aspects (quality, trust, security, integrity, and sovereignty) within the TN-ITS framework.

Each tool will be discussed in depth, focusing on its specific capabilities and contributions to improving data practices.



### 6.1.1. Identification of potential for certifications

After extensive discussions and research, it can be concluded that there is significant potential for stakeholder certification based on a trust list. This concept aligns, to some extent, with the approach of the Trust List Manager (TLM) certificates within the European Union C-ITS Security Credential Management System (EU CCMS)<sup>65</sup>.

A proposed diagram for trust certifications within the TN-ITS data chain (a simplified version of the C-ITS concept) was introduced to the group. However, it was decided not to include it in this report and instead prioritize its future development. It was anticipated that the initial phase of this idea could lead to confusion and significant disagreement among the readers. What was undertaken, as already mentioned in Section 5.3 (Trust Approach), was the creation and presentation of a form (sample) with the possible approach to Digital Contracts. These are legally binding agreements between organizations that define the terms and conditions for data sharing, including responsibilities, expectations, and penalties for non-compliance. In the context of TN-ITS, these contracts ensure that all parties involved in the data chain (e.g., road authorities, map providers, and ITS service providers) adhere to agreed-upon standards for data quality, security, and trust.

**Note:** A sample TN-ITS Trust Digital Contract is presented in Annex D.

### 6.5.1. Standardized metadata schema / DCAT-AP

DCAT-AP<sup>66</sup> (Data Catalogue Vocabulary Application Profile for Data Portals in Europe) is a standardized metadata schema developed by the European Commission. Its purpose is to enhance the interoperability, discovery, and sharing of datasets across various data portals in Europe. Built upon the W3C's DCAT (Data Catalogue Vocabulary), DCAT-AP provides a common framework for describing public sector datasets, making them easier to catalogue, find, and reuse across different platforms. Key components include Catalogue, Dataset, and Distribution, with a design that allows extensibility to meet specific needs while maintaining a consistent metadata structure. Widely adopted in European open data portals, DCAT-AP plays a crucial role in ensuring that public sector data is accessible and interoperable across different countries and regions.

The integration of DCAT-AP into the TN-ITS data chain introduces significant opportunities for enhancing the management and exchange of transport infrastructure data. TN-ITS focuses on the real-time exchange of transport infrastructure static updates, such as changes in road attributes or traffic signs. By applying DCAT-AP's standardized metadata schema to TN-ITS, stakeholders can benefit from improved data interoperability, discovery, and management across diverse systems and regions. Here are some benefits of implementing it in TN-ITS:

<sup>65</sup> European Commission, *C-ITS Certificate Policy Release: Preparatory Phase of Delegated Regulation 2019/1789*, (Luxembourg: Publications Office of the European Union, 2020), last accessed January, 2025, [https://cpoc.jrc.ec.europa.eu/data/documents/c-its\\_certificate\\_policy\\_release\\_preparatory\\_phase\\_of\\_Delegated\\_Regulation\\_2019\\_1789.pdf](https://cpoc.jrc.ec.europa.eu/data/documents/c-its_certificate_policy_release_preparatory_phase_of_Delegated_Regulation_2019_1789.pdf).

<sup>66</sup> DCAT -AP 3.0 latest release of DCAT-AP, June 2024, <https://semiceu.github.io/DCAT-AP/releases/3.0.0/>



- **Improvement of Data Quality:** DCAT-AP provides a structured, detailed, and consistent metadata framework that can significantly enhance the quality of data within the TN-ITS ecosystem. Standardizing how datasets are described, ensures that the data is well-documented, making it easier for stakeholders to assess accuracy, relevance, and provenance.
- **Enhancing Stakeholder Trust:** Standardizing metadata with DCAT-AP promotes trust among stakeholders, such as road authorities, map providers, and transport operators. Clear and consistent metadata ensures a shared understanding of the data, reducing the likelihood of misinterpretation or errors, and fostering confidence in the data exchange process.
- **Facilitating Data Governance and Sovereignty:** DCAT-AP aids in managing data governance by clearly defining data ownership, jurisdiction, and usage restrictions. This is crucial for maintaining control over data, ensuring compliance with local laws and regulations, and protecting data sovereignty in an increasingly interconnected digital environment.

However, not everything appears straightforward. Certain challenges are readily identified:

- **Metadata Standardization vs. Specific Needs of TN-ITS** - Aligning the generalized structure of DCAT-AP with the specific requirements of TN-ITS presents a significant challenge. Ensuring this alignment is essential for maintaining high data quality, as any gaps or inconsistencies in metadata can introduce inaccuracies. Misalignment can impact stakeholder trust, as discrepancies in metadata may raise concerns about the reliability and consistency of shared data.
- **Complexity in Maintaining Data Consistency** - Ensuring consistent and up-to-date metadata across different stakeholders is vital for both data quality and integrity. In TN-ITS, where data is constantly evolving, keeping metadata synchronized with actual data changes can be complex, risking the introduction of outdated or incorrect information. These issues directly impact trust and data quality, as fragmented data exchange or incomplete metadata may reduce the effectiveness of the TN-ITS system.
- **Data Governance and Sovereignty** - Managing data governance and sovereignty across multiple regions presents challenges, particularly in ensuring that data ownership and usage rights comply with local laws. This complexity affects both sovereignty and trust, as stakeholders must be confident that their data governance practices are robust and legally compliant.
- **Scalability and Performance** - As the TN-ITS network grows, scalability and performance issues could affect data quality and integrity. Delays or difficulties in updating metadata could lead to outdated information, compromising decision-making processes reliant on accurate and timely data.
- **Security and Privacy Concerns** - Although DCAT-AP does not directly address security, metadata can assist in implementing security practices. However, there is a risk that metadata might inadvertently expose sensitive information or become a target for unauthorized access. Maintaining robust security measures is essential to protect data integrity and sustain stakeholder trust.

- Cost and Resource Allocation - Implementing and maintaining DCAT-AP standards can be resource-intensive, particularly for smaller organizations. This challenge can impact data quality, trust, and sovereignty, as disparities in resource allocation might lead to uneven implementation and management across the TN-ITS network.
- Training and Stakeholder Engagement - Adequate training and engagement are essential for ensuring that all stakeholders correctly apply DCAT-AP standards. This affects both trust and data integrity, as consistent and accurate use of the standard is necessary to maintain reliable data across the network.

Integrating DCAT-AP with TN-ITS offers a powerful framework for enhancing data management, quality, and interoperability within transport networks. However, the challenges outlined from metadata standardization to governance and security must be carefully managed. Looking forward, as technologies like autonomous vehicles and 5G networks evolve, the role of DCAT-AP in supporting sophisticated, data-driven transport systems will become even more critical. Addressing these challenges now will lay the foundation for a more robust and resilient TN-ITS ecosystem in the future.

To address these challenges and leverage the strengths of DCAT-AP in TN-ITS the recommendations and Best Practices are as follows:

- Financial Support to Improve Stakeholder Engagement - Conduct workshops and training sessions to ensure all stakeholders understand and consistently apply DCAT-AP, thereby enhancing the effectiveness of the metadata system.
- Data Governance Policies - Establish clear governance policies that integrate DCAT-AP with TN-ITS needs, focusing on managing data quality, trust, security, sovereignty, and integrity across the network.
- Implementation Strategies – Implement a custom profile of DCAT-AP, such as **mobilityDCAT-AP**, that aligns with the specific requirements of TN-ITS and utilizes advanced metadata management tools to support continuous updates and automation.
- Metadata Standardization - In the context of the TN-ITS data chain, the adoption of a standardized metadata schema such as DCAT-AP not only enhances data interoperability but also plays a crucial role in the effective deployment of AI systems. As AI increasingly becomes integral to data processing and decision-making, ensuring that metadata schemas are designed with AI in mind is essential. This includes adherence to principles of transparency, explainability, and data integrity as recommended by ISO/IEC TR 24028:2020, which are key to maintaining trust in AI-driven processes.

#### 6.5.1.1. **mobilityDCAT-AP**

The NAPCORE Task 4.2.4 members fully support the implementation of mobilityDCAT-AP as a viable and strategic solution for enhancing the interoperability and standardization of mobility data across Europe. mobilityDCAT-AP is an extension of DCAT-AP developed within the framework of the NAPCORE project. Its primary objective is to adapt the DCAT-AP profile to better describe, and catalogue datasets related to mobility and transport, promoting



interoperability and data sharing across various platforms and national systems in the European Union. mobilityDCAT-AP was created to address the emerging need for harmonization and interoperability of National Access Points (NAPs) for mobility data, as mandated by the ITS Directive (2010/40/EU) and other related European policies. The NAPCORE project, which coordinates this effort, aims to ensure that mobility data is accessible and usable in a consistent manner across Europe, fostering an integrated digital mobility ecosystem.

Some relevant features of mobilityDCAT-AP to highlight based on the topics of this report are:

- Integration of the TN-ITS Format - One of the key features of mobilityDCAT-AP is the integration of the TN-ITS format within its catalogue. This allows real-time updates on transport infrastructure, such as changes in speed limits and traffic signs, to be described and shared in a standardized and interoperable manner. This facilitates the use of these data in various applications, including navigation systems and infrastructure management.
- Infrastructure Descriptors - Additional fields are provided to describe the relevant features of TN-ITS.
- Traffic and Public Transport Data - Capabilities to describe datasets that include information on traffic conditions, public transport, routes, and other essential data for the operation of transport systems using TN-ITS.
- Data Quality Element - Regarding data quality, mobilityDCAT-AP includes a specific element, but it is optional and in free text format. This element offers implementers the freedom to adopt the quality approach that best suits their needs, reflecting the fact that the definition and standardization of data quality is still an ongoing topic. This provides flexibility but also poses a challenge in ensuring the consistency and reliability of data.

The adoption of mobilityDCAT-AP brings significant benefits for the management and exchange of mobility data, including:

- Improvement in Data Quality - With standardized and detailed descriptions, mobility data can be better managed and reused, ensuring greater accuracy and relevance.
- Increased Trust Among Stakeholders - Using a common structure for data description fosters trust among different stakeholders, such as transport authorities, mobility service operators, and technology developers.
- Facilitation of Innovation - The interoperability facilitated by mobilityDCAT-AP supports the development of new intelligent mobility solutions, such as Mobility as a Service (MaaS) and connected and autonomous vehicles. Moreover, it provides a solid pillar of static data, specifically a static map layer containing precise physical attributes, which are up-to-date.

The integration of mobilityDCAT-AP with TN-ITS is highly relevant for the harmonization and interoperability of mobility data across Europe. With TN-ITS now integrated into the mobilityDCAT-AP catalogue, real-time updates on transport infrastructure can be described in a standardized way, making them easier to use by various stakeholders. mobilityDCAT-AP also allows flexibility (such as quality element) allowing data to be adapted to local needs but



requires a careful approach to ensure consistent data quality. Together, mobilityDCAT-AP and TN-ITS provide a solid foundation for the evolution of a more interconnected and efficient mobility ecosystem, aligned with European directives and policies.

### **Validation Tool for mobilityDCAT-AP**

To ensure the correct implementation and conformance of mobilityDCAT-AP, a validation tool is currently under development. This tool is designed to validate datasets against the mobilityDCAT-AP standards, helping implementers ensure that their data is compliant with the required specifications. The validation process leverages SHACL (Shapes Constraint Language) files, which define the constraints and structure expected for mobility data. This tool also provides a crucial resource for maintaining the quality and consistency of mobility data across platforms.

### **Metadata Conversion Tools for mobilityDCAT-AP Adoption**

Metadata conversion tools are essential for expediting the adoption of the mobilityDCAT-AP standard, as they automate the transformation of existing metadata formats into mobilityDCAT-AP-compliant structures. This streamlines the process for organizations, ensuring their mobility-related datasets are easily discoverable and interoperable.

Currently, while tools exist for general metadata conversion to standards like DCAT-AP, there is a need to develop specific transformation tools for the extension mobilityDCAT-AP. Such tools would greatly enhance interoperability and simplify the integration of various data schemas into the mobilityDCAT-AP framework, making it easier for organizations to adopt and align with this standard in the future.

## **6.5.2. Feedback loop tools**

In the context of the TN-ITS data chain, the feedback loop plays a critical role in ensuring the continuous improvement of data as clarified previously. Feedback loops can be essential in adaptive dynamic adjustments to new data, or changes in user requirements. To effectively manage and enhance these feedback loops, a set of tools is identified. These tools are designed to facilitate the collection, processing, and integration of feedback at various stages of the data chain, involving different stakeholders such as Data Holders, Data Users, Service Providers, Access Points, and End Users. Their involvement can also serve as distribution of the responsibility for data quality and integrity making the system more responsive to different stakeholders and thus more attractive for their data inputs.

Each tool is aligned with key data aspects, such as quality, trust, security, integrity, and sovereignty, ensuring that the feedback mechanisms contribute positively to the overall data governance. The benefit can be seen in early detection and correction which ensures that data sets are meeting the freshness and correctness at all stages. The following section provides a brief overview of these tools, including their descriptions, expected improvements and impacts, and potential challenges. This list aims to equip stakeholders with the necessary tools to implement effective feedback loops within the TN-ITS ecosystem, ultimately enhancing the

system's ability to respond to issues and improve its data-driven services. The performance of these tools can be significantly enhanced using AI models.

- a) **Feedback Management Tool:** An automated system that collects, analyses, and integrates feedback into decision-making workflows and dashboards, responding to the feedback originator to complete the loop.
- Motivation - Automates the collection and processing of feedback to ensure it is efficiently integrated into workflows.
  - Impact - Increases operational efficiency and ensures feedback is systematically and consistently addressed.
  - Challenges - This may require significant investment in technology and adaptation by users and data managers. Integrating with legacy systems can also be difficult.

In the TN-ITS data chain, a Feedback Management Tool could be used to collect feedback from data stakeholders, for example, road authorities, and analyse it. It can also identify issues with data quality, such as accuracy, timeliness, or security, and suggest a resolution. The feedback tool can also be used to track the effectiveness of changes made, which gives stakeholders insights into their feedback processing.

- b) **Reporting Tool:** A tool that enables End Users or Service Providers to report issues and provide feedback directly to Data Holders and Data Users. The tool can be accessed via APIs or graphical user interfaces (GUIs) of a mobile application or website.
- Motivation - Facilitates direct communication between users and data managers, allowing for quick issue resolution.
  - Impact - Improved data quality and reliability, increased end-user satisfaction, and faster resolution of issues.
  - Challenges - Ensuring all users have access to the tool and know how to use it effectively. Additionally, managing and prioritizing feedback can be challenging.
- c) **Public Consultations Tool:** A tool that organizes periodic public feedback sessions, such as seminars or targeted surveys, to gather insights into data usage and identify gaps.
- Motivation - Captures a broad range of feedback from end users and other stakeholders to improve services and data quality.
  - Impact - Better understanding of user needs and potential improvements in the services offered.
  - Challenges - Ensuring meaningful participation from stakeholders and efficiently analysing the large volumes of feedback that may be generated.
- d) **Compliance Assessment Incorporation Tool:** A tool that incorporates findings from compliance assessments, such as self-declarations, into the data chain.
- Motivation - Ensures processes meet established standards and regulations by integrating and verifying compliance into the data flow.
  - Impact - Increases trust and regulatory compliance, reducing the risk of penalties and improving data governance.

- Challenges - Ensuring all involved parties understand and adopt the necessary compliance practices.
- e) **Internal Feedback Tool:** A tool for exchanging specific feedback on data quality and format between Data Holders and Data Users. It can be manual (email/phone) or preferably automated (API).
- Motivation - Facilitates internal communication to ensure data quality issues are quickly resolved and that data meets user expectations.
- Impact - Enhances data quality throughout the chain, promoting a continuous flow of information and corrections.
- Challenges - Manual communication can be slow and prone to errors, while automation can be complex and costly to implement.

The feedback loop tools within the TN-ITS ecosystem are crucial for enhancing all the data aspects within the data chain. These tools enable effective communication and feedback integration across the data chain, involving all key stakeholders. By using these tools, feedback can be systematically processed and incorporated into workflows, improving data governance and overall system performance.

Feedback loop tools are essential for continuously improving the quality and reliability of the TN-ITS data chain. By incorporating AI, these tools can be enhanced to provide more efficient and automated feedback mechanisms, enabling real-time adjustments and improvements. To ensure that these AI-driven tools are trustworthy and reliable, it is important to design them following the guidelines set out in ISO/IEC TR 24028:2020, which emphasize transparency, explainability, and resilience in AI systems. This alignment will help maintain stakeholder trust while leveraging the full potential of AI in the feedback process.

The tools outlined in this chapter offer a framework for robust feedback loops, addressing issues quickly and enhancing user satisfaction. However, challenges such as accessibility, feedback management, and system integration need careful consideration. Moving forward, the success of these tools will depend on stakeholder collaboration to overcome these challenges, ensuring the TN-ITS ecosystem remains responsive, reliable, and focused on continuous improvement in data-driven services.

## 7. Use Case Analysis: Speed Limit

In this chapter, we will conduct a comprehensive analysis of the speed limit use case within the TN-ITS data chain framework. The purpose of this analysis is to illustrate how speed limit data is collected, processed, distributed, and utilized, highlighting the various ITS roles and data aspects involved. By exploring these aspects, this chapter will not only enhance understanding of how speed limit data is managed within the TN-ITS framework but also contribute to the development of potential tools and methodologies aimed at promoting and ensuring the quality, trust, integrity, sovereignty, and security of such data.

### 7.1. Motivation for Selecting the Speed Limit Use Case

When the objective is the identification of potential measures to improve all the referred aspects and within the previously established considerations, the definition of use cases is of high importance. Carefully structured use cases lead to an elevated understanding of scenarios, an improved overall overview of the processes and stakeholders (particularly their involvement throughout the data-chain stages), and possibly the identification of potential inefficiencies and how to mitigate them.

TN-ITS is focused on the exchange of updates on road data attributes such as traffic signage (e.g., warnings and restrictions, roadworks, road closures), lane information, and speed limits. TN-ITS devotes particular attention to the standardized data exchange between road authorities (providers of these data) and map makers and service providers. ITS-related road data exchange at the EU level directly influences road safety and efficiency.

Additionally, we adopted this authoritative speed limit data (use case) because of the need to comply with the ISA related regulations from the EC.

**Note:** Since subsection 7.4 provides a highly detailed and extensive analysis based on the speed limit use case, it was agreed to keep subsections 7.2 and 7.3 more generic to allow for future analysis of other use cases.

### 7.2. Requirements and Expectations

Given the importance of understanding the dynamics involved at each stage of the TN-ITS data chain, it is crucial to analyse how stakeholders—namely Data Holders, Data Users, Access Points, Service Providers, and End-Users (as defined in Delegated Regulation 2022/670)—engage with their respective roles. This analysis provides insights into the involvement of each stakeholder across the data chain stages, the specific data aspects they influence, and the tools and processes they employ.

The **Stakeholder-Centric Approach** applied in this analysis serves several critical purposes:

- Stage Involvement - Identifying at which stage of the data chain (data collection, processing, exchange, integration, and usage) each stakeholder is involved.
- Level of Involvement - Assessing the depth of each stakeholder’s involvement at these stages, whether direct or indirect.



- Influence on Data Aspects - Determining which data aspects Quality, Trust, Integrity, Security, and Sovereignty are directly influenced by the stakeholder's involvement at each stage.
- Processes and Tools Utilization - Exploring the processes, strategies, mechanisms, and tools used or potentially utilized by each stakeholder to optimize their roles within the data chain, thereby enhancing overall data quality and system integrity.
- Tool Application Across Stages - Advising on the stages of the data chain where the application of specific assessment tools is most effective.

### 7.3. Analysis Procedures

This analysis was conducted collaboratively by the active members of Task 4.2.4 of the NAPCORE project. The work was initially organized in Excel format, allowing for detailed cross-referencing and mapping of the above elements before being formalized into this report. The procedures followed include:

#### 1. Integration of Data Aspects Across Stages:

- Procedure: Integrate the key data aspects—Quality, Trust, Integrity, Security, and Sovereignty—across the stages of the data chain. Evaluate how these aspects are managed by each stakeholder at each stage, identifying synergies and potential gaps.
- Purpose: To ensure that each data aspect is effectively maintained throughout the data lifecycle, contributing to the overall reliability and robustness of the TN-ITS data chain.

#### 2. Cross-Analysis of Stakeholder Roles and Responsibilities:

- Procedure: Conduct a cross-analysis of each stakeholder's roles and responsibilities concerning the data stages. This includes assessing how each stakeholder's involvement impacts the management of data aspects and ensuring a clear delineation of responsibilities.
- Purpose: To optimize the role of each stakeholder within the data chain, ensuring effective collaboration and minimizing risks associated with role ambiguity or redundancy.

#### 3. Tool Application and Effectiveness Review:

- Procedure: Review the tools identified during the analysis for their effectiveness in managing data aspects at various stages. Evaluate the appropriateness of these tools for each stakeholder and stage and identify opportunities for improving or adopting new tools.
- Purpose: To ensure that the tools in use are effective and appropriately applied, enhancing the overall efficiency and integrity of the data chain.

#### 4. Feedback Loop and Continuous Improvement Evaluation:

- Procedure: Analyse the effectiveness of feedback loops and monitoring mechanisms, focusing on how feedback from end-users and other stakeholders is integrated to drive continuous improvement.



- **Purpose:** To ensure that the data chain remains adaptive and responsive to feedback, allowing for ongoing improvements in data quality, trust, integrity, and security.

**5. Synthesis of Findings into Actionable Insights:**

- **Procedure:** Synthesize the analysis findings into actionable insights that inform strategic planning and decision-making for the TN-ITS data chain. These insights are designed to enhance the performance and resilience of the system.
- **Purpose:** To provide clear, actionable recommendations for stakeholders, helping them optimize their roles, refine processes, and implement tools more effectively.

**6. Documentation and Reporting of Analytical Outcomes:**

- **Procedure:** Compile the outcomes of the analysis into this comprehensive report, transitioning from the detailed Excel work to a formal document. This process includes documenting strengths, weaknesses, and opportunities identified.
- **Purpose:** To provide a transparent and thorough record of the analysis, serving as a reference for future audits, process improvements, and strategic developments within the TN-ITS framework.

**7.4. Data Chain stage and Stakeholders analysis**

The TN-ITS data chain is designed in such a way that every individual stakeholder is encountered with one or more role(s) in part of the five data chain stages and the feedback loop process. The following analysis and respective tables display the involvement the roles/stakeholders have on data aspects per data chain stage and the feedback loop.

**Note:** If the relationship is too indirect or if there is no involvement in a particular stage of the data chain, it will not be mentioned in the role analysis. It was also decided to limit the analysis to a maximum of two stages per data aspect to avoid making the text overly exhaustive.

**7.4.1. Data holders – speed limit analysis**

Data Holders, such as road authorities, are pivotal in managing and updating road infrastructure data, including road attributes like speed limits and road signage (equipment). They are directly responsible for collecting, verifying, and maintaining this data, ensuring its accuracy, consistency, and reliability before sharing it with other stakeholders in the TN-ITS data chain. The identified stakeholders for the Data Holder role are road authorities fulfilling systematic management, updates, and maintenance of digital (machine-readable) records of road infrastructure changes, such as speed limit signs.

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Quality</b> (of data)	<b>Data Collection:</b> A road authority monitors and updates data on changes in the speed	<b>Data Collection:</b> Data range checks to verify speed limits, and quality-check logs



Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
	limit, ensuring accuracy within the national limits. <b>Data Processing:</b> The authority may also validate the data before sharing it with the data user.	to track data accuracy. Define and create precise work procedures that establish a structured approach to data collection, which eventually maintains or increases data quality; Alternative: Incorporate machine learning-based anomaly detection tools that can automatically identify and flag outliers or inconsistencies in data. <b>Data Processing:</b> Administrative tools for data verification and quality control, ensuring data consistency before forwarding it to the NAP operator.
<b>Trust</b> (on Stakeholder)	<b>Data Collection:</b> Trust is established by adhering to Standard Operating Procedures (SOPs) directives during data collection. <b>Feedback Loop:</b> Feedback from service providers and end-users is used to improve data accuracy and maintain trust.	<b>Data Collection:</b> Self-assessment tools to ensure SOP compliance, potentially certified by an independent body. <b>Feedback Loop:</b> Verification tools for cross-referencing feedback with third-party sources, ensuring reliability and accuracy.
<b>Integrity</b> (of data)	<b>Data Collection:</b> Ensuring that all changes in data are logged, including who made the changes, is crucial for data integrity. <b>Data Processing:</b> Monitoring integrity during data handling and processing, ensuring no unauthorized changes are made.	<b>Data Collection:</b> Data access logs to monitor changes and identify responsible parties. <b>Data Processing:</b> Internal audit systems to verify data integrity during and after processing stages.
<b>Security</b> (on data)	<b>Data Collection:</b> Implementing security measures to protect the data at the point of collection. <b>Data Exchange:</b> Ensuring secure data transmission to Data Users and Access Points.	<b>Data Collection:</b> Authentication and authorization mechanisms to secure data inputs. <b>Data Exchange:</b> Encryption services and secure transmission protocols to protect data in transit.
<b>Sovereignty</b> (of the data)	<b>Data Processing:</b> Classifying data based on sensitivity (public, internal, confidential) and ensuring appropriate access controls. <b>Feedback Loop:</b> Managing compliance with SLAs and licenses, particularly when breaches are identified through feedback.	<b>Data Processing:</b> Tools for data classification based on ISO standards. <b>Feedback Loop:</b> SLA/licenses compliance monitoring, including regular audits and classification reviews.

Table 20 - Data Holders: Speed Limit Analysis of Use Cases and Potential Assessment Tools (by Data Stage)

#### 7.4.2. Data Users – speed limit analysis

Data Users, which may include the road authority itself, road operators, tolling operators, service providers, digital map producers, or any other entity using static road data to keep real-time traffic information up-to-date, play a key role in processing and publishing road infrastructure data. These stakeholders are responsible for various stages, including data



collection, processing, exchange, and feedback loops, with a primary focus on transforming raw data into standardized formats like TN-ITS while maintaining the integrity, quality, and security of the data. Although a direct identification of a specific data user was not necessary in this case, their role in improving data quality will be a key focus of our analysis.

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Quality</b> (of data)	<p><b>Data Collection:</b> Data Users retrieve data from the road authority’s database and must ensure its quality before processing.</p> <p><b>Data Processing:</b> The data is processed into a standardized TN-ITS format, ensuring it meets all quality standards.</p>	<p><b>Data Collection:</b> Data access checks to ensure the reliability of the retrieved data.</p> <p><b>Data Processing:</b> TN-ITS validators, syntax-check tools, and version checks to guarantee data accuracy and compliance with standards.</p>
<b>Trust</b> (on Stakeholder)	<p><b>Data Processing:</b> Validating the quality of data received from the Data Holders before further processing to build and maintain trust.</p> <p><b>Feedback Loop:</b> Data Users participate in feedback loops to address data quality issues and improve trust.</p>	<p><b>Data Processing:</b> Verification tools to ensure data quality before publishing, self-assessment tools for adherence to processing standards. Alternative: Introduce third-party audits.</p> <p><b>Feedback Loop:</b> Tools for processing and acting on feedback to continuously improve data trustworthiness.</p>
<b>Integrity</b> (of data)	<p><b>Data Processing:</b> While converting data to TN-ITS format, Data Users ensure integrity by adding digital signatures and maintaining logs.</p> <p><b>Data Exchange:</b> Ensuring that data integrity is preserved during the exchange process.</p>	<p><b>Data Processing:</b> Digital signature tools to certify data integrity, and data change logs to track modifications. Alternative: Implement blockchain-based solutions to track and verify all data changes.</p> <p><b>Data Exchange:</b> Metadata updates and integrity verification tools to preserve data authenticity during transmission.</p>
<b>Security</b> (on data)	<p><b>Data Exchange:</b> Implementing security protocols during data exchanges, such as encrypted transmissions and secure authentication processes.</p> <p><b>Data Processing:</b> Ensuring that security measures are applied consistently throughout the data processing stage.</p>	<p><b>Data Exchange:</b> Authentication, Authorization &amp; Accounting Services, and encryption protocols to protect data during exchanges.</p> <p><b>Data Processing:</b> Secure processing environments with access control and data encryption measures.</p>
<b>Sovereignty</b> (of the data)	<p><b>Data Processing:</b> Ensuring that data processing respects SLAs and legal agreements, with appropriate metadata updates to reflect ownership and usage rights.</p> <p><b>Feedback Loop:</b> Continuously monitoring SLA compliance through feedback mechanisms to ensure sovereignty is maintained.</p>	<p><b>Data Processing:</b> SLA/licenses integration into metadata, tools for legal compliance tracking.</p> <p><b>Feedback Loop:</b> Compliance tracking tools for monitoring adherence to sovereignty requirements.</p>

Table 21 - Data Users: Speed Limit Analysis of Use Cases and Potential Assessment Tools (by Data Stage)

### 7.4.3. Access Point – speed limit analysis

For this use case, we focus our analysis on the member state as the stakeholder responsible for setting up access points, such as NAPs, where datasets, services, and metadata related to the data listed in the RTTI Delegated Regulation Annex are made accessible for re-use. The Access Point, established by the member state, acts as a hub where road infrastructure data, such as speed limits, is published and made accessible to authorized users. It plays a crucial role in several stages, including data processing, exchange, and feedback loops, ensuring that the data remains secure, trustworthy, and compliant with legal standards. Thus, the use case can be adapted to ensure that “Changes to the speed limit data must be properly published on the NAP.”

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Quality</b> (of data)	<p><b>Data Exchange:</b> Ensuring that data-exchanging services are reliable by performing regular IT infrastructure audits. Alternative: implement real-time monitoring of the data exchange infrastructure to ensure consistent service availability.</p> <p><b>Feedback Loop:</b> Collecting user feedback to identify and rectify any data quality issues.</p>	<p><b>Data Exchange:</b> IT infrastructure audit tools, and compliance assessments to ensure data exchange reliability.</p> <p><b>Feedback Loop:</b> User feedback tools for collecting and addressing data quality concerns.</p>
<b>Trust</b> (on Stakeholder)	<p><b>Data Exchange:</b> Trust is ensured by verifying that the metadata includes certifications and trust-related information from Data Holders.</p> <p><b>Feedback Loop:</b> Continuously gathering feedback on trust-related issues to improve data reliability.</p>	<p><b>Data Exchange:</b> Trust certification tools, and metadata verification systems to ensure trustworthiness.</p> <p><b>Feedback Loop:</b> Feedback tools for capturing and analysing trust-related concerns.</p>
<b>Integrity</b> (of data)	<p><b>Data Exchange:</b> Verifying the legitimacy of data users through metadata checks, ensuring that data integrity is preserved.</p> <p><b>Feedback Loop:</b> Monitoring feedback to identify and address any integrity issues that arise.</p>	<p><b>Data Exchange:</b> Legitimacy checks, digital signature verification tools.</p> <p><b>Feedback Loop:</b> Integrity monitoring tools based on user feedback and metadata analysis.</p>
<b>Security</b> (on data)	<p><b>Data Exchange:</b> Implementing robust security protocols for data exchange, including encryption and authentication, to establish a secure environment.</p>	<p><b>Data Exchange:</b> Authentication, Authorization &amp; Accounting Services, encryption frameworks to protect data during transmission.</p> <p>Alternative: Implement a zero-trust architecture that requires continuous verification of access.</p>
<b>Sovereignty</b> (of the data)	<p><b>Data Exchange:</b> Ensuring that metadata includes SLA and license information to manage and enforce data sovereignty.</p>	<p><b>Data Exchange:</b> Metadata management tools for SLA/license integration.</p> <p><b>Feedback Loop:</b> Compliance tracking and SLA monitoring systems.</p>

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
	<b>Feedback Loop:</b> Addressing feedback related to sovereignty issues to ensure compliance with legal standards.	

Table 22 - Access Point: Speed limit analysis of Use Cases and Potential Assessment Tools (by Data Stage)

#### 7.4.4. Service Providers – speed limit analysis

Service Providers, such as map providers, integrate road infrastructure data like speed limits into their mapping systems, playing a crucial role in data exchange, integration, usage, and feedback loops. The speed limit use case is tailored to ensure that these map producers integrate data about changes in speed limits into their systems. They can also send feedback to the data user and/or data holder regarding the accuracy, reliability, format, and timeliness of the data, helping to improve its quality throughout its lifecycle while providing updated services to end-users. When a service provider receives feedback from End-Users directly of any discrepancies in speed limits, it is also recommended for the service provider to validate this input carefully, ensuring the legitimacy and relevance of the feedback received. This selection process helps to filter out invalid inputs not to be elevated further and allows the data user and/or data holder to focus on actionable and accurate information.

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Quality</b> (of data)	<p><b>Data Exchange:</b> Retrieving updated speed limit data from the data exchange and validating its accuracy before integration.</p> <p><b>Data Integration:</b> Integrating the validated data into mapping systems, ensuring it is accurate and up to date.</p>	<p><b>Data Exchange:</b> TN-ITS XML Validation Tool, semantic and syntactic validation tools. Alternative: Introduce AI-driven semantic validation tools that can understand the context and detect more complex inconsistencies.</p> <p><b>Data Integration:</b> Additional data checks and integration tools to ensure data quality during system updates.</p>
<b>Trust</b> (on Stakeholder)	<p><b>Data Integration:</b> Service Providers validate the trust credentials of Data Holders and Data Users before integrating their data.</p> <p><b>Feedback Loop:</b> Continuously validating trust through feedback mechanisms and user interactions.</p>	<p><b>Data Integration:</b> Trust certification and verification tools, continuous monitoring systems.</p> <p><b>Feedback Loop:</b> Feedback loop processing tools, and trust monitoring systems.</p>
<b>Integrity</b> (of data)	<p><b>Data Integration:</b> Verifying the integrity of data by checking digital signatures and metadata before integrating it into systems.</p> <p><b>Data Exchange:</b> Ensuring integrity is maintained during the exchange process.</p>	<p><b>Data Integration:</b> Digital signature verification tools, and provenance checks.</p> <p><b>Data Exchange:</b> Metadata updates and integrity verification tools.</p>

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Security</b> (on data)	<b>Data Exchange:</b> Implementing security protocols to secure data during the exchange and integration processes. <b>Data Integration:</b> Ensuring secure data storage and access control within mapping systems.	<b>Data Exchange:</b> Authentication, Authorization & Accounting Services, encryption protocols. <b>Data Integration:</b> Secure storage solutions, and access control systems.
<b>Sovereignty</b> (of the data)	<b>Data Integration:</b> Respecting SLAs and licenses during data integration, with appropriate metadata updates reflecting ownership and usage rights.	<b>Data Integration:</b> Metadata update tools for SLA/license integration, and compliance management systems.

Table 23 - Service Providers: Speed Limit Analysis of Use Cases and Potential Assessment Tools (by Data Stage)

#### 7.4.5. End-Users – speed limit analysis

Within the use case of speed limit changes on roads, the end-user is defined as the driver using a navigation system or a mobile application. End-users or drivers are the first to experience any discrepancies that may arise in real-world scenarios. They rely on the accuracy and timeliness of road infrastructure data provided by Service Providers and are primarily involved in the data usage and feedback loop stages. Their feedback is crucial for identifying discrepancies and eventually improving the overall quality, trust, and reliability of the data. By obtaining feedback directly from End-users, inputs can be gathered across various road classes, broadening the geographic coverage of the feedback.

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Quality</b> (of data)	<b>Data Usage &amp; Feedback Loop:</b> Using navigation systems with updated speed limit data and reporting any inaccuracies found.	<b>Feedback Loop:</b> Feedback reporting tools, in-app error reporting systems. Alternative: Implement advanced user feedback systems with real-time reporting and AI-driven analysis to prioritize and address issues more effectively.
<b>Trust</b> (on Stakeholder)	<b>Feedback Loop:</b> By providing the possibility to give continuous feedback on navigation services, End-Users help to maintain and increase trust in the service providers. Engage the End-User in the chain to “make them feel” they are part of the system.	<b>Feedback Loop:</b> Service usage feedback tools, and trust rating systems.
<b>Integrity</b> (of data)	<b>Feedback Loop:</b> Reporting inconsistencies in data during usage, which are then addressed by service providers.	<b>Feedback Loop:</b> Integrity monitoring tools based on user feedback, and automated error detection systems.
<b>Security</b> (on data)	<b>Data Usage:</b> Securing access to navigation services through authentication processes to ensure that data is legitimate and secure.	<b>Data Usage:</b> Authentication and authorization tools, continuous security monitoring systems.

Data Aspect	Example/Use Case (by relevant Stage)	Potential Assessment Tools (by Stage)
<b>Sovereignty</b> (of the data)	<b>Feedback Loop:</b> End-Users indirectly support data sovereignty by ensuring their feedback helps maintain data accuracy and compliance with legal standards.	<b>Feedback Loop:</b> Privacy dashboards, user consent management tools, and data control features.

Table 24 - End Users: Speed Limit Analysis of Use Cases and Potential Assessment Tools (by Data Stage)

## 7.5. Analysis Reflections and Strategic Insights

This section encapsulates the key findings from conducted analysis and provides insight into the broader implications for the TN-ITS data chain. It underscores the importance of implementing the suggested recommendations to achieve an optimal system while acknowledging that the current state of the TN-ITS data chain may not fully align with these ideal conditions.

### Key Findings

- **Robust Foundation:** The TN-ITS data chain is fundamentally robust, with clearly defined roles and responsibilities for each stakeholder. The process for managing essential data aspects is well-structured, providing a solid foundation for data management.
- **Effectiveness of Existing Tools:** The tools currently employed are generally effective, particularly in maintaining critical aspects like data quality and security. These tools ensure that the TN-ITS data chain operates smoothly and reliably, contributing to the overall success of the framework.
- **Opportunities for Enhancement:** Despite its strengths, there are several areas where the TN-ITS data chain could be optimized. These include:
  - **Tool Diversification:** Implementing a broader range of tools, particularly those that leverage advanced technologies like blockchain for data integrity or AI for real-time monitoring, could significantly enhance the system's capabilities.
  - **Cross-Stakeholder Collaboration:** Strengthening collaboration between stakeholders, particularly in feedback loops and data exchange processes, would improve overall data quality and trust across the chain.
  - **Real-Time Monitoring Systems:** The introduction of real-time monitoring tools would allow for more proactive management of data aspects, enabling stakeholders to address issues as they arise rather than reacting after the fact.

### Overall Implications

- **Enhanced Effectiveness and Reliability:** By addressing these areas for improvement, stakeholders can significantly enhance the effectiveness and reliability of the TN-ITS data chain. Implementing the recommended tools and processes would lead to substantial gains in data quality, trust, integrity, security, and sovereignty. This, in turn, would ensure that the system remains robust and resilient in the face of evolving challenges.
- **Adaptability and Resilience:** The continuous evolution of the TN-ITS data chain, driven by stakeholder feedback and technological advancements, is crucial for maintaining



the relevance and effectiveness of the framework. By staying adaptable and resilient, the TN-ITS data chain can better meet the needs of its users and respond to new demands and threats.

The use case of the speed limit feedback loop presented previously, particularly where feedback is collected from End-Users, could be interpreted as an example of a ‘bottom-up’ approach. For instance, when discrepancies are detected by ISA systems between camera-detected speed limits and digital map data. There, conflicts are reported back to the service provider which then elevates it further to the data users and/or data holders, enabling updates and corrections based on actual conditions. This End-Users driven feedback ensures ground-level inconsistencies, such as damaged signs or outdated data, are addressed accordingly, enhancing accuracy over time.

When combined with the ‘top-down’ approach such as METR, where updated information from regulatory authorities is translated, certified, and disseminated in a standardized, machine-readable format, the two approaches would create a robust and complementary data chain. METR ensures consistency and authoritative dissemination of regulations, while the ISA feedback loop provides continuous refinement and real-world validation. Together, they could potentially form a dynamic system that ensures speed limit data remains accurate, reliable, and timely, supporting both conventional vehicle drivers and autonomous vehicles.

The ultimate success of the TN-ITS data chain depends on the collective commitment of all stakeholders to uphold and continuously improve data management standards. While the current system is strong, embracing the recommendations provided here will allow stakeholders to transform the TN-ITS data chain into a model of excellence in road infrastructure data management.

By prioritizing continuous improvement, fostering collaboration, and adopting advanced tools, stakeholders can ensure that the integrity and trustworthiness of the data chain are maintained over the long term. This proactive approach will not only secure the TN-ITS framework’s success today but also safeguard its future effectiveness in an increasingly complex and data-driven world.

## 8. Conclusions and recommendations

The overarching objectives of Task 4.2.4 included researching the most suitable quality system for TN-ITS services, drawing insights from EU-EIP D4.1, developing and implementing a data quality assessment methodology, and advancing concepts and mechanisms for data quality evaluation and enrichment tools. To effectively address these, this milestone (M4.2.7) focused on delivering on the commitments defined in Milestone 4.2.6.

M4.2.7's specific goals were to propose integrated approaches by leveraging various components and services, such as:

- Quality Criteria (level of Services and Data Quality Criteria) listed from TN-ITS GO, the EU ITS Platform (EU-EIP), and the 5-star rating system suggested by the latest Traveller Information Services Association (TISA).
- Data Aspects analyses: Trust, Quality, Integrity, Security, and Sovereignty.
- The Feedback Loop Tool: Build upon the TN-ITS Data Chain Feedback loop diagram from M4.2.6 by refining key areas to demonstrate the roles, stages, and feedback mechanisms within the data chain.
- Cooperative Models: Applying the cooperation principles from the Traffic Management 2.0 (TM2.0) project.

Furthermore, the team had worked on defining and refining the data aspects, stakeholders' roles, and identifying potential assessment tools and best practices to be employed throughout the data chain stages.

It is also worth noting that while developing this milestone, some data aspects had considered the use of the speed limit use case, while others did not. Which can leave some gaps in the analysis. This can be remedied by future actions building upon this milestone and incorporating the use case in further analyses.

### 8.1. Key contributions of M4.2.7

Milestone 4.2.7 analyses data aspects of trust, quality, integrity, security, and sovereignty within the data chain it proposes. It introduces guidelines and tools for evaluating and maintaining high quality, harmonising data through supporting better compliance with standards like the EU ITS Directive 2010/40/EU (consolidated version including amendments of Directive 2023/2661/EU) and the EU RTTI Delegated Regulation 2022/670 (amending EU Regulation 2015/962) as well as highlighting the roles of public road authorities and private service providers in maintaining data quality and consistency.

A major contribution of M4.2.7 is the improvement of the feedback loop process introduced in M4.2.6. This milestone further defines how feedback can be integrated into the TN-ITS Data Chain, suggests possible scenarios for its incorporation, and identifies its origin as well as how stakeholders will process it. M4.2.7 continues by introducing a use case focused on speed limits and how each Data Chain stage and stakeholder involved interact with the data. Furthermore, M4.2.7 recognises that other groups and initiatives like the RTTI Taskforce are also working on their versions of what a feedback loop process could look like. The



cooperation with these groups is vital for coming up with the strongest and most accurate feedback loop process possible.

M4.2.7 also discusses the use of evaluation frameworks like the TISA 5-star rating system, as a way of ensuring that data meets the quality levels they define. This supports the EU's Intelligent Speed Assistance (ISA) regulation (DR(EU) 2019/2144) by providing accurate, timely, and reliable speed signs in digital maps. These efforts directly improve road safety and traffic efficiency while aligning with mobility goals. Even more, by highlighting and analysing potential recommended tools for evaluating these aspects (quality, trust, integrity, security, and sovereignty) of data that stakeholders will interact with, M4.2.7 helps ensure higher standards within the data chain.

### 8.1.1. TN-ITS and DATEX II Alignment SWOT Analysis

As previously mentioned, the task group agreed that a presentation of potential concerns regarding the alignment between TN-ITS and DATEX II standards should be included in the conclusions chapter. These concerns should be considered as key aspects that both communities should closely monitor in the future.

The alignment of DATEX II and TN-ITS<sup>67</sup>, acts as a key step, presenting a strategic opportunity to strengthen transportation data management across Europe by integrating two established frameworks. The process of technical alignment and standardization work has been initiated and is ongoing. A comparative analysis<sup>68</sup> has been conducted to evaluate the elements of both frameworks. Several technical alignments have already been discussed within both communities, including areas such as, but not limited to, the following:

1. Alignment with the CEN specification number 16157, *part 11: Publication of machine interpretable traffic regulations*, ensuring smooth integration of TN-ITS with DATEX II part 11, which deals with traffic regulations such as speed limits and road condition changes.
2. Changes needed in DATEX II parts (*Part 1: Context and Framework & Part 7: Common Data Elements*), the adjustment needed so that the TN-ITS data can be better integrated into the DATEX II system.

While the technical aspect of the alignment is outside the scope of this current report, as mentioned in Chapter 1.3, a contribution can be made by analysing the strategic planning aspect of the alignment. Overseeing this convergence in a more holistic and comprehensive manner.

Given the relevance and critical importance of this topic for the future of TN-ITS, the Task 4.2.4 group has chosen to make a meaningful contribution by including in this report several concerns that should be carefully considered by both communities during the process of aligning standards. To this end, an email was distributed to both communities, inviting input on potential concerns that may arise during the alignment process regarding the five data

---

<sup>67</sup> DATEX II, *DATEX II and TN-ITS converge for enhanced traffic services interoperability*, February 2024, <https://datex2.eu/2024/02/05/datex-ii-and-tn-its-merge-for-enhanced-traffic-services-interoperability/>

<sup>68</sup> DATEX/TN-ITS Session at MDD 2024, November /2024, <https://www.napcore.eu/documents/MDD2024ppt/19datex.pdf>



aspects studied in this report: quality, trust, security, integrity, and sovereignty. This proactive approach aims to ensure a comprehensive understanding of potential challenges and foster collaboration in addressing them effectively.

Therefore, a SWOT analysis was conducted to examine its **Strengths**, **Weaknesses**, **Opportunities**, and potential **Threats**, based on data gathered from multiple publicly available sources in addition to our views, providing insight into its significance<sup>69</sup> and the challenges<sup>70</sup> that may emerge from the convergence of the two frameworks.

**Note:** Please note that the SWOT analysis and TOWS matrix were conducted based on the information presently available. However, this is not limited to what has been provided, as the process is ongoing. It is inevitable that new strengths, weaknesses, opportunities, and threats may arise, which will also need to be considered further.

This SWOT analysis reflects important aspects to consider for ensuring a smooth adoption and implementation of the alignment process between DATEX II and TN-ITS.

- **Strengths (Internal):**

TN-ITS focuses on static data, while DATEX II deals with dynamic data, making their convergence complementary. This integration enables **streamlined data exchange**, making processes more efficient and with common standards and formats reducing manual intervention. Furthermore, the framework enhances the **accuracy and timeliness** of transport data, ensuring up-to-date information on various interfaces. To continue it can improve the **reliability** of applications that heavily depend on transport data and enhance **interoperability**, facilitating seamless data exchange between different systems and stakeholders. Finally, both data standards are highlighted as the preferred standards for transport data in the RTTI Delegated Regulation further supporting their alignment.

- **Weaknesses (Internal):**

Despite its potential, convergence faces several challenges, including the **technical complexities** of integrating data and ensuring **compatibility** with existing systems. For example, addressing governance would require aligning both technical elements (such as bug reporting, bug tracking, schema files, repository, etc.) and non-technical elements (such as governance communities, governance of standard, formal standardization, training, legal structure, website, etc.) between the two frameworks. The **implementation costs** may also create barriers for some stakeholders, especially for those who already have a running service.

- **Opportunities (External):**

<sup>69</sup> ERTICO, *TN-ITS consolidated the merger with DATEX II at the 9<sup>th</sup> DATEX II User Forum*, October 2024, <https://erticonetwork.com/tn-its-consolidated-the-merger-with-datex-ii-at-the-9th-datex-ii-user-forum/>

<sup>70</sup> Ken Spiteri Gili, *The Convergence of TN-ITS and DATEX II: Enhancing Interoperability in Transport Data*, March 2024, [https://www.linkedin.com/pulse/convergence-tn-its-datex-ii-enhancing-transport-data-ken-spiteri-gili-uvvdf?trk=article-ssr-frontend-pulse\\_more-articles\\_related-content-card#:~:text=safety%2C%20and%20sustainability.,Challenges,-and%20Considerations](https://www.linkedin.com/pulse/convergence-tn-its-datex-ii-enhancing-transport-data-ken-spiteri-gili-uvvdf?trk=article-ssr-frontend-pulse_more-articles_related-content-card#:~:text=safety%2C%20and%20sustainability.,Challenges,-and%20Considerations)



The alignment framework can **drive innovation** by offering a standardized foundation for developing advanced technologies, particularly for connected and automated vehicles. The framework can also promote **collaboration between the public and the private sectors** while maintaining **consistent data quality principles** across the EU. An aligned framework may also be more **flexible** and agile in integrating emerging technologies, such as AI, 5G, and CCAM technologies. The alignment of standards also could potentially **increase adoption and trust** among stakeholders, encouraging collaboration. Additionally, this alignment could **reduce regulatory fragmentation**, enabling the European Commission and governments to establish clear and consistent policies. Furthermore, such alignment would position the initiative as a global **leader**, setting a new benchmark with the potential for long term influence.

- **Threats (External):**

Successful implementation will require addressing several threats, including ensuring **compliance with regulatory requirements**, at a European or National level. Additionally, overcoming **stakeholder resistance**, and managing the potential **lack of awareness or expertise** among diverse stakeholders during the adoption process are critical. **Cybersecurity risks** also pose a significant threat, as the complexity of integration might bring up vulnerabilities in the systems. Finally, the **slow pace of adaptation** could jeopardise its relevance, especially given the fast-paced technological advancements.

DATEX II & TN-ITS Alignment	Advantages	Hindrances
Internal	<b>Strengths:</b> <ul style="list-style-type: none"> <li>- Streamlined data exchange</li> <li>- Improve accuracy and timeliness</li> <li>- Enhances reliability</li> <li>- Support greater interoperability</li> </ul>	<b>Weaknesses:</b> <ul style="list-style-type: none"> <li>- Addressing technical complexities</li> <li>- Addressing compatibility</li> <li>- Addressing governance matters (technical &amp; non-technical elements)</li> <li>- Implementation costs</li> </ul>
External	<b>Opportunities:</b> <ul style="list-style-type: none"> <li>- Driving innovation</li> <li>- Promote collaboration between public and private sectors</li> <li>- Consistent data quality</li> <li>- Greater flexibility for future adaptations (AI-based)</li> <li>- Increased adoption and trust</li> <li>- Simplified regulation</li> <li>- Global leadership positioning of the alignment</li> </ul>	<b>Threats:</b> <ul style="list-style-type: none"> <li>- Ensuring compliance with legal challenges (National and European level)</li> <li>- The challenge in engaging stakeholders</li> <li>- Lack of awareness or expertise among stakeholders</li> <li>- Cybersecurity risks</li> <li>- The slow pace of adaptation</li> </ul>

Table 25- DATEX II & TN-ITS Alignment SWOT Analysis

From the SWOT analysis above, we can then take further steps to identify actions from the findings obtained, by identifying the TOWS matrix. The TOWS matrix identifies important



points for further action by trying to anticipate weaknesses, minimize threats, and make the most of the strengths to maximize opportunities. The following is the description of each component of the TOWS matrix, followed by Table 26 which shows the TOWS matrix of the DATEX II & TN-ITS alignment,

**SO (Strengths & Opportunities):** What strengths can be used to optimise the opportunities?

- **Leverage streamlined data exchange to drive innovation and simplify regulation.** The aligned framework has the potential to facilitate the development of advanced technologies, such as AI-based traffic management or autonomous vehicle communications, by using efficient data exchange with common standards and formats. Efficient standardised data handling can also simplify regulatory compliance by reducing administrative burden and ensuring consistent processes across all stakeholders.
- **Improve accuracy and timeliness to enhance trust, collaboration, and consistent data quality.** Increasing the accuracy and timeliness of transportation data can build trust among stakeholders, which is essential for enhancing collaboration between public and private sectors. Reliable and up-to-date transportation data will also ensure consistency in data quality.
- **Support interoperability to increase adoption, trust, and leadership positions.** The alignment of standards and specifications between TN-ITS and DATEX II promotes interoperability in transportation data exchange, thereby enhancing seamless data exchange between systems and stakeholders. This interoperability will enable broader adoption, build trust, and as adoption increases, strengthen the initiative's leadership position by setting the standard for the transportation data exchange framework.
- **Leverage reliability and interoperability to ensure flexibility for future adaptation.** The reliability and interoperability of the aligned framework ensures that the framework will remain relevant to emerging technologies such as CCAM, and AI integration. This will demonstrate that the framework can adapt to future needs and remain scalable for the future.

**WO (Weaknesses & Opportunities):** What weaknesses must be tackled to optimize the opportunities?

- **Address technical complexities to drive innovation and increase flexibility for future adaptation.** Addressing technical complexity related to data integration and system compatibility is critical to driving innovation. This complexity needs to be addressed so that the framework can more effectively integrate emerging technologies such as AI and CCAM, making sure it remains flexible and adaptable for future advancements.
- **Address compatibility issues to encourage greater collaboration and maintain consistent data quality.** Addressing compatibility between the two frameworks should ensure that different systems can work together seamlessly. This will facilitate stronger collaboration between public and private sector stakeholders, as they can rely on consistent, high-quality data. Ensuring that all systems are compatible will also increase trust, driving wider adoption and collaboration.

- **Addressing governance matters (technical & non-technical) to increase adoption, and trust.** The key challenge is aligning governance matters across the technical (e.g. schema, bug tracking, repositories, etc.) and non-technical (e.g. legal, community, training, etc.) aspects of the frameworks. By addressing these governance issues, the framework can support better collaboration and encourage wider adoption.
- **Integrating AI to address technical complexity and improve data generation interfaces.** Engaging AI experts and utilising their input to design human-natural interfaces to generate data can help simplify complex technical elements. AI-driven interfaces can automate certain technical aspects, making it easier for stakeholders to generate and interpret data without requiring deep technical expertise. This approach can address the technical complexities of data integration and open up the possibility for innovative AI-based solutions in transportation.

**ST (Strengths & Threats):** What strengths can be used to better handle the threats?

- **Leverage streamlined data exchange to ensure regulatory compliance.** By using streamlined data exchange processes and common standards, the alignment framework can help ensure compliance with national and European regulatory requirements. Integration of standard formats simplifies data reporting, making it easier to meet legal standards and minimises the risk of non-conformities that could lead to disputes over intellectual property or usage rights.
- **Use greater accuracy and timeliness to engage stakeholders and raise awareness.** Accurate and timely data can help overcome the challenges of stakeholder resistance and lack of awareness. By providing up-to-date and reliable data, the framework can build trust and show the value of the system. This encourages stakeholders to adopt the system and participate more actively, overcoming barriers related to lack of expertise or reluctance to engage.
- **Increase reliability to reduce cybersecurity risks.** System reliability, ensured by strong technical standards, can help reduce cybersecurity risks. Reliable and well-structured systems are generally more secure and less prone to vulnerabilities. By building a strong and reliable framework, the chances of cyber threats or breaches can be reduced, helping to protect sensitive data and maintain stakeholder trust.
- **Promote interoperability to accelerate adaptation and overcome slow adaptation.** Improved framework interoperability ensures that diverse systems can work together seamlessly. This is critical in addressing slow adaptation threats, as it enables faster integration of new technologies. Interoperable systems can more easily adapt to evolving standards, ensuring the framework remains relevant and adaptable to new technologies and requirements.

**WT (Weaknesses & Threats):** What weaknesses can be addressed to overcome external threats?

- **Address technical complexity to ensure compliance with regulatory requirements.** The technical complexity involved in integrating different systems can create barriers to compliance with national and European regulations. By addressing this complexity early in the integration process (such as through better data mapping, standardised

interfaces, and clear technical documentation), the framework can help prevent incompatibilities that could lead to legal disputes over data use or intellectual property rights.

- Address compatibility and governance matters to better engage stakeholders.** Addressing compatibility between the TN-ITS and DATEX II, as well as aligning governance matters (both technical and non-technical), will help overcome stakeholder resistance. A clear governance framework, with well-defined rules, bug tracking, schema files, legal structures, etc. can make it easier for stakeholders to understand how to engage with the system. This alignment helps raise awareness, educate stakeholders, and overcome resistance, ultimately leading to greater collaboration.
- Manage implementation costs to minimise cybersecurity risks.** By carefully managing implementation costs, the framework can free up resources to invest in cybersecurity measures, ensuring that vulnerabilities are not introduced due to rushed or poorly funded integration. Proper budgeting for cybersecurity can help safeguard the framework from potential threats, ensure data security, and build trust among stakeholders, which are essential to long-term success.
- Strengthen governance and technical alignment to accelerate adaptation.** A major threat is the slow pace of adaptation due to governance and technical challenges. By aligning the technical and non-technical elements of governance, the framework can ensure that all stakeholders are on the same page, thereby accelerating the adaptation process. With clear guidelines and reduced ambiguity, stakeholders will find it easier to adopt the system and adapt it to their needs.

DATEX II & TN-ITS Alignment	Strengths	Weaknesses
<b>Opportunities</b>	<p><b>SO (Strengths &amp; Opportunities):</b></p> <ul style="list-style-type: none"> <li>- Leverage streamlined data exchange to drive innovation and simplify regulation</li> <li>- Improve accuracy and timeliness to promote trust, collaboration, and consistent data quality</li> <li>- Support interoperability to increase adoption, trust, and leadership positioning</li> <li>- Leverage reliability and interoperability to ensure flexibility for future adaptations</li> </ul>	<p><b>WO (Weaknesses &amp; Opportunities):</b></p> <ul style="list-style-type: none"> <li>- Address technical complexities to drive innovation and enhance flexibility for future adaptations</li> <li>- Address compatibility issues to promote greater collaboration and maintain consistent data quality</li> <li>- Addressing governance matters (technical &amp; non-technical) to increase adoption, trust, and leadership positioning</li> <li>- Integrating AI to address technical complexities and improve data generation interfaces</li> </ul>
<b>Threats</b>	<b>ST (Strengths &amp; Threats)</b>	<b>WT (Weaknesses &amp; Threats):</b>

	<ul style="list-style-type: none"> <li>- Leverage streamlined data exchange to ensure regulatory compliance</li> <li>- Use greater accuracy and timeliness to engage stakeholders and raise awareness</li> <li>- Increase reliability to reduce cybersecurity risks</li> <li>- Promote interoperability to accelerate adaptation and overcome slow adaptation</li> </ul>	<ul style="list-style-type: none"> <li>- Address technical complexity to ensure compliance with regulatory requirements</li> <li>- Address compatibility and governance issues to better engage stakeholders</li> <li>- Manage implementation costs to minimize cybersecurity risks</li> <li>- Strengthen governance and technical alignment to speed up adaptation</li> </ul>
--	--	--

Table 26 - DATEX II & TN-ITS Alignment TOWS Matrix

### 8.2. Deployment plan/roadmap

The deployment roadmap for M4.2.7 includes both immediate and long-term goals for improving data management. Initially, it focuses on implementing feedback loop tools and standardizing metadata through frameworks like mobilityDCAT-AP to improve data compatibility. Developing APIs for real-time validation and error detection also helps address quality issues quickly.

Medium-term goals should include aligning TN-ITS with DATEX II and introducing unified licensing frameworks to make road authorities’ data openly accessible. With the continuation of NAPCORE’s goals through NAPCORE-X, we can exploit the opportunity to further define and enhance the relationship between TN-ITS and DATEX II to ensure the harmonisation between the two standards. Stakeholders will use evaluation tools and metrics to monitor and improve data quality consistently. Regular training and workshops will help build knowledge and support the adoption of best practices.

In the long term, the plan aims to create a centralized repository for traffic management data and guidelines. This will promote information sharing and consistent implementation of the TN-ITS framework.

### 8.3. Potential Recommendations

To improve the management of traffic regulations across EU Member States, a structured, multi-step approach is required. This should begin with detailed surveys and investigations to understand the varying practices each Member State employs for managing road data. Given that each MS often has multiple road authorities, their methods for handling and reporting data to the TN-ITS data chain differ significantly. The initial focus should be on mapping existing traffic regulations, identifying inconsistencies, and ensuring alignment with standards like TN-ITS to establish a strong basis for improvement. A critical step in this process is the development of a refined Data Chain framework that clearly defines the stages, roles, and information flows. This framework will enhance interoperability and provide a structured methodology for integrating diverse national approaches into a cohesive European-wide system.



Variations in administrative processes among Member States and regional authorities often result in different formats and standards for issuing traffic regulations. To harmonize these differences, it is essential to establish clear processes for managing and use of traffic regulation order data. Each stage of the data chain must adhere to recognized standards to ensure consistent quality and interoperability. The alignment between TN-ITS and Datex II plays a key role in standardization. A structured analytical approach is offered in this report to assess the advantages, disadvantages, and concerns associated with aligning these standards, focusing on data quality, trust, security, integrity, and sovereignty.

A key step toward achieving consistency in traffic regulation management is defining authoritative data requirements. Authoritative data provides a legally recognized framework, ensuring that critical traffic management information, such as speed limits, meets high-quality standards. This reinforces trust and reliability within the data chain (e.g. TN-ITS data chain), benefiting all stakeholders. To strengthen this process, the recommendation for the application of Quality Criteria and Levels of Quality in RTTI proposes a comprehensive quality assessment model, integrating TN-ITS GO, EU-EIP, and the TISA 5-star rating system as benchmarks. By leveraging these criteria, road authorities can enhance data accuracy, reliability, and interoperability.

To maintain consistency and compliance, data quality tools and metrics should be applied to assess the contributions of road authorities. Key focus areas include timeliness, accuracy, and adherence to standards. The ISA (Intelligent Speed Assistance) implementation serves as a practical use case, allowing map providers to benefit from controlled testing environments, as outlined in the TISA ISA Guideline paper. By integrating structured quality frameworks, enhanced feedback loops, cooperative trust models, and a refined data chain framework, TN-ITS can significantly improve the management and interoperability of traffic regulation data across the EU.

To safeguard the data chain, it is essential to address potential vulnerabilities in data handling, different data aspects. Implementing a set of recommended tools will help mitigate risks by addressing various data-related challenges, ensuring a secure and resilient data exchange process. Additionally, leveraging Traffic Management 2.0 (TM2.0) cooperative principles, the new Cooperative (Trust) Models proposal fosters collaboration, transparency, and trust among stakeholders. By applying these principles, data chains, such as TN-ITS, can strengthen relationships between road authorities, map providers, and policymakers, ensuring a more integrated and harmonized approach to data sharing.

Establishing feedback mechanisms is crucial for maintaining and enhancing data quality. These mechanisms should incorporate both user input and automated systems to detect and address errors, ensuring that traffic regulation lifecycles are continually refined. Given the unique administrative frameworks and localized requirements of each MS, these feedback mechanisms must be flexible yet robust to accommodate national differences while maintaining overall consistency. To support this, the recommended Feedback Loop Tool expansion refines stakeholder roles, process stages, and feedback mechanisms, ensuring continuous quality improvement in RTTI data flows. This approach builds upon the TN-ITS GO Project Feedback Loop, reinforcing transparent and effective data governance across the EU.



#### **8.4. Future steps**

Future work can help address challenges faced by the TN-ITS framework. Finalizing the agreement between TN-ITS and DATEX II is essential to unify data standards and improve system compatibility throughout the MS. It is also possible that technologies like artificial intelligence and machine learning can further support data validation and prediction, ensuring road authority data remains useful and accurate. With technological changes sure to take place in the future, this further complicates implementation. Keeping the TN-ITS framework aligned with emerging tools and standards requires balancing immediate needs with long-term planning.

Expanding feedback loops to include real-time feedback from end-users and systems like the fused map-camera suggestion by TISA, can further help in improving the accuracy of the data in the data chain. Furthermore, the creation of a bank of guidelines and best practices can help standardize implementation across Member States. This can encourage broader adoption of the TN-ITS framework. One of the next steps will also involve understanding the level of technological investment to be adopted and the associated costs, depending on the scenarios and options presented in this report.

It is also important to take into consideration the significance of training sessions with stakeholders. These sessions can give participants the knowledge needed to manage traffic data effectively. Future scaling pilot projects and creating evaluation frameworks will measure how these improvements impact road safety, traffic efficiency, and data quality.

## 9. Annexes

**Annex A** - Identified TN-ITS Data-Chain Tools; Criteria analysis: Level of implementation complexity (technical), Level of impact/Importance, Level of Feasibility (organization/legal), and Business Prospect.

(Please note that the definitions of the tools and their respective associations with the data aspects, TN-ITS roles, and data-chain stages can be found in the subchapter “Identification of Data Evaluation Tools”)

Categories	Name of Tool	Level of complexity (technical) (1,3,5,7,9 -> low to high)	Level of Impact / Importance (1,3,5,7,9 -> low to high)	Level of organization/legal complexity (1,3,5,7,9 -> low to high)	Business prospect (immediate & mid-term)	Weighted average of all criteria	%
<b>Semantic Validation Tools</b>	Data type & enumeration checks	3	7	3	Immediate	5,5	78,57
	Version check	3	7	3	Immediate	5,5	78,57
	Data type & enumeration checks (Service)	1	7	3	Immediate	5,9	84,29
	Version check (Service)	1	7	3	Immediate	5,9	84,29
	Range checks	7	5	5	Immediate	3,6	51,43
<b>Syntactic Validation Tools</b>	TN-ITS (XML) Validation Tool	3	7	5	Immediate	5	71,43
	TN-ITS (XML) Validation Tool (FME)	3	7	5	Immediate	5	71,43
	TN-ITS (XML) Validation Tool (Service)	3	5	5	Immediate	4,4	62,86
<b>Compliance Assessment</b>	Compliance Assessment tool - Declaration of Compliance	7	9	7	Mid-Term	4,175	59,64
<b>Security Audits</b>	ISO 27001	5	7	5	Mid-Term	4,475	63,93
	Common Criteria (EUCC ISO 15408)	7	7	9	Mid-Term	3,075	43,93
	Authorization ABB	5	9	5	Immediate	5,2	74,29
	Node Authentication ABB	5	9	5	Immediate	5,2	74,29



This project has received funding from the European Commission’s Directorate General for Transport and Mobility under Grant Agreement no. MOVE/B4/SUB/2020-123/SI2.85223

<b>Authentication, Authorisation &amp; Accounting Services</b>	Data Encryption ABB (XML-Enc as a possible extension)	7	5	7	Mid-Term	<b>2,975</b>	<b>42,50</b>
	Non-Repudiation ABB	5	5	5	Mid-Term	<b>3,875</b>	<b>55,36</b>
	Data Integrity ABB	5	7	7	Mid-Term	<b>3,975</b>	<b>56,79</b>
	Data Provenance ABB	7	5	9	Mid-Term	<b>2,475</b>	<b>35,36</b>
	Access-Log: The web server generates an access log tool	3	5	3	Mid-Term	<b>4,775</b>	<b>68,21</b>
	Change-log tool	3	7	3	Mid-Term	<b>5,375</b>	<b>76,79</b>
	Certified List	7	7	9	Immediate	<b>3,2</b>	<b>45,71</b>
<b>Standardized metadata schema</b>	DCAT-AP (mobilityDCAT-AP)	5	9	5	Mid-Term	<b>5,075</b>	<b>72,50</b>
<b>Feedback Loop</b>	Reporting Tool	5	9	3	Immediate	<b>5,7</b>	<b>81,43</b>
	Feedback Management Tool	5	7	5	Mid-Term	<b>4,475</b>	<b>63,93</b>
	Public Consultations	3	5	3	Mid-Term	<b>4,775</b>	<b>68,21</b>
	Assessment Incorporation Tool	5	5	5	Mid-Term	<b>3,875</b>	<b>55,36</b>
	Internal Feedback	5	9	5	Immediate	<b>5,2</b>	<b>74,29</b>
<b>Service/Administrative Tools</b>	SLA / Licenses	3	7	5	Immediate	<b>5</b>	<b>71,43</b>
	Audits	5	7	5	Mid-Term	<b>4,475</b>	<b>63,93</b>
	Digital Signature	5	7	7	Immediate	<b>4,1</b>	<b>58,57</b>
	Trust Certification	7	9	9	Immediate	<b>3,8</b>	<b>54,29</b>

## Annex B - Integrating Data Aspects into Vulnerability Clustering

Data Chain Stage	Main Vulnerability	Secondary Vulnerabilities	Trust	Quality	Integrity	Security	Sovereignty	Impact (%)
Data Collection	Incorrect data input	Data tampering	1	1	1	1	0,5	4,5
		Human Error	1	1	1	0,5	0	3,5
		Sensor inaccuracies (outdated equipment)	1	1	1	0,5	0	3,5
		Phishing	1	0,5	1	1	0,5	4
		Inadequate coverage	0,5	1	0,5	0	0	2
		Data provenance	1	1	1	0,5	1	4,5
Data Processing	Incorrect processes or data values	Algorithmic biases	1	1	1	0,5	0	3,5
		Erroneous data transformations	1	1	1	0,5	0	3,5
		Supply-chain attacks	0,5	0,5	1	1	1	4
		Inadequate data anonymization techniques	1	1	1	1	1	5
		Computational resource limitations	0,5	1	0,5	0	0	2
Data Exchange	Malicious Data Injection	Unauthorized access	1	0,5	1	1	1	4,5
		Data leakage	1	0,5	1	1	1	4,5
		Malware	1	0,5	1	1	1	4,5
								73
								72
								90

	<b>Lack of standardization</b>	Insecure Transmission Protocols	1	1	1	1	1	5	87
		Outdated metadata	1	1	1	0,5	0,5	4	
		Inconsistent metadata	1	1	1	0,5	0,5	4	
<b>Data Integration</b>	<b>Incorporating wrong data into the maps</b>	Data compatibility issues	1	1	1	0,5	0,5	4	80
		Conflicting data schemas	1	1	1	0,5	0,5	4	
		Poor data mapping techniques	1	1	1	0,5	0,5	4	
		Semantic heterogeneity	1	1	1	0,5	0,5	4	
<b>Data Usage</b>	<b>Display false or wrong information</b>	Data misinterpretation	1	1	1	0,5	0	3,5	75
		Improper utilization of context	1	1	1	0,5	0	3,5	
		Biased decision-making	1	1	1	0,5	0	3,5	
		Lack of User Training	1	1	1	0,5	0	3,5	
		Misleading Visualizations	1	1	1	0,5	0	3,5	
		Denial-of-service (DoS, DDoS)	1	0,5	1	1	1	4,5	
		Ransomware attacks	1	0,5	1	1	1	4,5	
		Lack of transparency	1	1	1	0,5	0	3,5	
		<b>Importance</b>	<b>27,5</b>	<b>25,5</b>	<b>28</b>	<b>18,5</b>	<b>13</b>		
<b>%</b>	<b>95</b>	<b>88</b>	<b>97</b>	<b>64</b>	<b>45</b>				

## Annex C - Identifying Key Stakeholders for Countermeasure Implementation

Secondary Vulnerabilities	Potential Countermeasures	Stakeholder major responsibility				
		Data Holders	Data Users	Access Point	Service Providers	End Users
Data tampering	Implement strong data authentication mechanisms to detect unauthorized modification. Use digital signatures or cryptographic hashing to ensure data integrity and prevent tampering.	1	0,5	0,5		
Human Error	Regular training of personnel to minimize human errors.	1	0,5			
Sensor inaccuracies (outdated equipment)	Regular maintenance and updating of sensor equipment and frequent calibration of sensors to ensure accuracy.	1				
Phishing	Security awareness training to identify and avoid phishing attacks. Implement multi-factor authentication to protect access.	1	1	0,5		
Inadequate coverage	Conduct coverage studies to identify areas with inadequate coverage. Invest in technology to expand coverage where necessary.	1				
Data provenance	Implement a data provenance tracking system to ensure the authenticity of data sources. Regularly audit the data custody chain.	1	0,5	0,5	0,5	
Algorithmic biases	Regularly audit algorithms to detect and correct biases. Use diverse and balanced datasets for algorithm training.	0,5	1			
Erroneous data transformations	Implement a multi-stage validation process to detect and correct inconsistencies with regular review and audit data transformations to ensure accuracy.	0,5	1	0,5	0,5	
Supply-chain attacks	Continuously monitor suppliers to detect early signs of attacks. Conduct cybersecurity assessments and regular security audits of suppliers.	0,5	1			

Inadequate data anonymization techniques	Adopt robust data anonymization techniques such as k-anonymity, l-diversity, or differential privacy. Regularly test anonymization methods to ensure that data cannot be reidentified.	1	1			
Computational resource limitations	Implement resource monitoring tools to identify and mitigate bottlenecks. Plan and allocate sufficient computational resources for peak processing times.	1	0,5			
Unauthorized access	Implement strict access controls and multi-factor authentication to prevent unauthorized access by regularly monitoring and log access attempts to detect suspicious activities.		0,5	1		
Data leakage	Encrypt data both in transit and at rest to safeguard it from leakage. Implement Data Loss Prevention (DLP) tools and monitor for potential leaks.	0,5	1	1	0,5	
Malware	Deploy advanced malware detection and prevention systems, including endpoint protection solutions. Regularly update and patch systems to mitigate vulnerabilities.	0,5	1	1	0,5	
Insecure Transmission Protocols	Use secure transmission protocols such as TLS/SSL to protect data exchange. Conduct regular security testing, including penetration tests, to identify and resolve protocol vulnerabilities.	0,5	1	1	0,5	
Outdated metadata	Establish and enforce metadata standards across the stakeholders. Regularly review and update metadata to ensure it remains current and consistent.	1	1	1		
Inconsistent metadata	Implement a centralized metadata management system to maintain consistency. Perform regular audits to identify and correct metadata inconsistencies.	1	1	1	0,5	
Data compatibility issues	Implement rigorous data validation processes to detect compatibility issues. Use middleware solutions to facilitate interoperability between different systems and formats.		1	0,5	1	
Conflicting data schemas	Standardize data schemas across the stakeholders to prevent conflicts. Regularly audit and harmonize data schemas to ensure alignment.	0,5	1	0,5	1	
Poor data mapping techniques	Use standardized data mapping practices and tools and continuously review and refine data mapping techniques to enhance accuracy.	0,5	1	0,5	1	
Semantic heterogeneity	Develop and implement ontologies and data dictionaries to ensure semantic alignment across systems and utilize semantic integration tools that support automatic mapping and translation of data semantics.	0,5	1	0,5	1	
Data misinterpretation	Provide user training and clear documentation on correct data interpretation practices. Implement data visualization tools that highlight uncertainties and provide context.		0,5	0,5	1	
Improper utilization of context	Implement decision support tools that correctly integrate and present contextual data.			0,5	1	

Biased decision-making	Regularly audit decision-making processes to identify and mitigate bias.	0,5	1		1	
Lack of User Training	Develop comprehensive, ongoing training programs for users to ensure they are equipped to use data correctly. Regularly assess and update training materials to cover emerging challenges and knowledge gaps.	0,5	1	1	1	
Misleading Visualizations	Validate all visualizations for accuracy and clarity before they are shared with end-users.		0,5	1	1	
Denial-of-service (DoS, DDoS)	Deploy DDoS mitigation services and scalable infrastructure to handle high traffic volumes. Monitor network activity continuously to detect and respond to DoS attacks promptly.		0,5	0,5	1	
Ransomware attacks	Maintain regular, secure backups of critical data to enable quick recovery from ransomware attacks. Implement comprehensive cybersecurity measures, including next-gen firewalls and anti-ransomware tools.	0,5	0,5	1	1	
Lack of transparency	Establish and communicate a clear data transparency policy to users. Use transparency tools that allow users to trace data origins and understand data limitations.	1	0,5	1	1	
<b>Stakeholder with major responsibility in the data chain</b>		<b>17</b>	<b>21</b>	<b>15,5</b>	<b>15</b>	<b>0</b>
<b>Stakeholder Impact in all Data Chain</b>		<b>60,71</b>	<b>75,00</b>	<b>55,36</b>	<b>53,57</b>	<b>0,00</b>

## Annex D – Digital Contract for TN-ITS Data Sharing

### Digital Contract for TN-ITS Data Sharing

Contract ID: TN-ITS-DATA-2025-001

Version: 1.0

Effective Date: January 01, 2025

#### 1. Parties to the Contract

Party A: Road Authority of [Country/Region], hereinafter referred to as "Road Authority," whose principal address is [Address].

Party B: [Service Provider Name], hereinafter referred to as "Service Provider," whose principal address is [Address].

#### 2. Purpose

This agreement establishes the terms for providing TN-ITS data-sharing services by the Service Provider to the Road Authority, ensuring timely, accurate, and reliable data for traffic management and decision-making.

#### 3. Scope of Services

The Service Provider agrees to:

1. Provide TN-ITS data, including but not limited to (outlined in Appendix I):
  - Speed limit
  - Road works
2. Ensure data delivery via a secure API.
3. Maintain service quality following the Service Level Agreement (Appendix II).

The Road Authority agrees to:

1. Use the data solely for traffic management purposes.
2. Ensure compliance with data access and security protocols.

#### 4. Payment Terms

- Service Fee: The Road Authority shall pay [amount in Euros] per month.
- Payment Schedule: Monthly, within 15 days of receiving the invoice.
- Late Payment Penalty: 2% of the overdue amount per month.

#### 5. Service Level Agreement (SLA)

*Please note that these SLAs are examples and will be used as needed with varying levels of detail according to the Quality levels. Trust levels and Security guarantees.*

##### 5.1 Quality - SLA

Outlined in Appendix II, the SLA specifies:

- Minimum uptime: 99.9%.

- Data delivery latency:  $\leq 5$  seconds.
- Data accuracy:  $\geq 98\%$ .
- Support response time for critical issues:  $\leq 30$  minutes.

Failure to meet SLA targets will result in service credits as detailed in Appendix II.

## 5.2 Security - SLA

Outlined in Appendix III.

## 5.3 Trust - SLA

Outlined in Appendix IV, the SLA specifies:

- Data privacy and security
- Legal and regulatory compliance
- Technical compatibility (can be specified in/as the Security SLA)
- Data quality and integrity (can be specified in/as the Quality SLA)

## 6. Data Privacy, Ownership, and Intellectual Properties Rights

The Road Authority retains ownership of all traffic data provided under this agreement. The Service Provider shall not use or disclose data for any purpose other than delivering the agreed-upon services. Both parties shall comply to:

- Compliance with EU Data Regulations
- Compliance with Data Anonymization Measures, where applicable
- Compliance with licensing terms related to data use and redistribution

## 7. Data Retention, Disposal and Incident Response

The Service Provider shall not retain the data beyond the agreed duration and delete it securely as agreed upon. Agreed upon measures should be taken in case of a data breach under the incident response plan.

- Retention Period: Specify how long the data can be retained by the recipient.
- Data Disposal: Detail the procedures for securely deleting or returning the data once the purpose of the contract has been fulfilled.
- Breach Notification: Outline the procedures for reporting data breaches, including the timeline and contact points.
- Incident Response Plan: Define the actions that will be taken in the event of a data breach, including mitigation measures and cooperation with authorities.

## 8. Term and Termination

The duration of the contract is specified to be:

- Duration:

This contract may be terminated under the following conditions:



1. Breach of contract terms, with a 30-day rectification period.
2. Persistent failure to meet SLA metrics for three consecutive months.

Both parties are bound to comply with any post-termination obligation as specified in Appendix V.

## 9. Dispute Resolution

Any disputes arising from this agreement will be resolved through arbitration in [City, Country], under the laws of [Jurisdiction].

## 10. Digital Signatures

This contract is executed digitally, and both parties agree to use legally recognized digital signatures under [eIDAS/ESIGN Act or applicable law].

Party A: Road Authority	Party B: Service Provider
Name: [Authorized Representative]	Name: [Authorized Representative]
Title: [Title]	Title: [Title]
Date: [Date]	Date: [Date]
Digital Signature: [Placeholder]	Digital Signature: [Placeholder]

## Appendices of Annex D

### Appendix I: Data Type

*Please note that these data types are used as examples.*

Types of Data	Data Categories	Format	Transmission
Timestamp	Metadata	ISO 8601 (e.g., YYYY-MM-DDTHH:MM:SSZ)	Secure API (HTTPS)
Road Segment ID	Spatial Data	UUID/String TN-ITS	Secure API (Initial Batch Upload)
Road Name	Spatial Data	WKT (Well-Known Text)	File Upload (GeoJSON/XML)
Speed Limit	Regulatory Data	Integer (km/h) TN-ITS	Initial Batch Upload
Traffic Sign Data	Regulatory Data	UTF-8 Text/Image URL	Batch File (JSON/XML)

## Appendix II: Quality Service Level Agreement (SLA)

*Please note that the SLA details are an example and should be adapted for each case.*

SLA Metric	Target	Penalty
Data Accuracy	≥ 98%	Service credit: 5% monthly fee for < 98%
Data Delivery Latency	≤ 5 seconds	Service credit: 10% monthly fee for > 5 secs
System Uptime	99.9%	1% credit per 0.1% drop below 99.9%
Support Response Time	Critical: 30 mins; Non-critical: 4 hours	Escalation to senior support for breaches

## Appendix III: Trust Service Level Agreement (SLA)

*Additional SLA information can be documented here, see Quality SLA as an example.*

## Appendix IV: Security Service Level Agreement (SLA)

*Additional SLA information can be documented here, see Quality SLA as an example.*

## Appendix V: Termination Obligations

*Additional information can be documented here.*