TN-ITS Inventory on requirements related to trust, quality, integrity, security and sovereignty of data

Contribution from Sub-Working Group 4.2

Status: Final
Version: 1.0
Date: 29 August 2023

Document information

Project acronym	NAPCORE
Full project title	National Access Point Coordination Organisation for Europe
Grant Agreement No.	MOVE/B4/SUB/2020-123/SI2.852232
Activity no. and title	4.2.4 TN-ITS enhancements concerning the data sharing supply chain
Author(s)	Georgios Christou – KIOS CoE, Cyprus
Co-author(s)	Madiha Shahzad, Rodolfo Da Silva - KIOS CoE, Cyprus, Frank Daems ERTICO
Related to Milestone No.	M 4.2.6
External Milestone	Yes

Document history

Version	Date	created/ modified by	Comments
Draft	01.06.2023	Madiha Shahzad - KIOS CoE, Cyprus Georgios Christou - KIOS CoE, Cyprus Rodolfo Da Silva - KIOS CoE, Cyprus	Initial version
0.1	14-6-2023	Frank Daems - ERTICO	Review remarks V0.1
0.1	25-7-2023	Madiha Shahzad - KIOS CoE, Cyprus Georgios Christou - KIOS CoE, Cyprus Rodolfo Da Silva - KIOS CoE, Cyprus	First draft of Chapters 1, 2, 3 and 4
0.1	01-08-2023	Frank Daems - ERTICO Stephen T'Siobbel – ERTICO Prisca Numbisi – ERTICO Edwin 't Lam - National Roads and Waterways Administration, Finland Miho Ishii – Trafikverket, Sweden	First draft revision
0.2	04-08-2023	Madiha Shahzad - KIOS CoE, Cyprus Georgios Christou - KIOS CoE, Cyprus Rodolfo Da Silva - KIOS CoE, Cyprus	Second version
0.2	08-08-2023	Frank Daems - ERTICO Stephen T'Siobbel - ERTICO	Second version revision
0.3	10-08-2023	Madiha Shahzad - KIOS CoE, Cyprus Georgios Christou - KIOS CoE, Cyprus Rodolfo Da Silva - KIOS CoE, Cyprus	Third version
0.3	27-08-2023	Benjamin Witsch - AustriaTech, Austria Damaris Gruber - AustriaTech, Austria Hana Peters - Rupprecht Consult GmbH	Third version revision
0.4	28-08-2023	Madiha Shahzad - KIOS CoE, Cyprus Rodolfo Da Silva - KIOS CoE, Cyprus	Fourth version
1.0	29-08-2023	Georgios Christou - KIOS CoE, Cyprus	Final version

Action Requested

☐ To be revised by partners involved in the preparation of the document

☐ For review/ approval by the Core Alignment Team

☒ For approval by the NAPCORE Steering Committee

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

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

1. Identification of trust, quality, integrity, security and sovereignty: This step involves research on data trust, quality, integrity, security and sovereignty mechanisms.
2. Research on state of the art existing optimal quality systems.
3. The TN-ITS Data Chain introduction. Additionally, vulnerabilities and potential attacks based on the TN-ITS data chain are assessed.
4. Inventory of requirements and collection of methodologies to mitigate vulnerabilities and potential attacks.

The report provides a comprehensive overview of the work carried out in the respective task and it is associated with Milestone M4.2.6. This version of the deliverable is the first draft, and the final version is expected in M4.2.7.

Abbreviations

Abbreviation	Meaning
ADAS	Advanced Driver Assistance Systems
CCAM	Cooperative Connected Automated Mobility
CEN	European Committee for Standardization
CWA	Closed World Assumption
DATEX II	DATa EXchange between traffic and travel information centers
DDoS	Distributed Denial of Service
DG Connect	Directorate-General for Communications Networks, Content and Technology
DG INFSO	Directorate-General for Information Society and Media (former DG-Connect)
EC	European Commission
eMaPS	eSafety Digital Maps Public Private Partnership Support Action
EMDS	European Mobility Data Space
ERTICO ITS Europe	European Road-transport Telematics Implementation Coordination Organisation
EU	European Union
EU-EIP	EU ITS Platform
EU-EIP D4.1 (Sub-Activity)	Determining Quality of European ITS Sevices
EuroNCAP	The European New Car Assessment Programme
EuroRAP	The European Road Assessment Programme
ETSC	European Transport Safety Council
GDF	Geographic Data Files
GML	Geography Markup Language

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

Abbreviation	Meaning
ICT	Information and communications technology systems
ID Devices	Identification devices to track vehicles
INSPIRE	Infrastructure for Spatial Information in the European Community
IoT	Internet of Things
ISA	Intelligent Speed Assist
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
OAuth	Industry-standard protocol for authorization
MS	Member States
NAP	National Access Point
NAPCORE	National Access Point Coordination Organisation for Europe
NAPCORE WG3 (T3.2)	WG3 (NAP Content and Accessibility) / T3.2 (Task Quality Frameworks)
NAPCORE SWG4.2 (T4.2.4)	SWG4.2 (TN-ITS) / T4.2.4 (TN-ITS Enhancements concerning the data sharing supply chain)
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)”
NPRA	Norwegian Public Road Administration
OADF	Open Autodrive Forum
OCL	Object Constraint Language
OWA	Open World Assumption
REST	REpresentational State Transfer
ROSATTE	Road Safety Attributes Exchange Infrastructure in Europe
RTTI	Real-Time Traffic Information
SENSORIS	SENSOR Interface Specification
SLA	Service Level Agreement
SWG	Sub Working Group
TEN-T	Trans-European Transport Network
TN-ITS	Transport Network Intelligent Transport Systems: www.tn-its.eu
TN-ITS GO	TN-ITS sub-project
UML	Unified Modelling Language
WG	Working Group
XML	eXtensible Markup Language Format
XSD	XML Schema Definition

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

Table of Contents

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

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

1. Introduction

The work on Transport Network - Intelligent Transport Systems (TN-ITS) deliverable, titled, "TN-ITS Inventory on requirements related to trust, quality, integrity, security and sovereignty of data" consists of the following subtasks:

1. Establishing a technical expert team with the National Access Point Coordination Organisation for Europe (NAPCORE) Member States (MS) and TN-ITS community.
2. Researching and creating an inventory of data trust-related items and mechanisms.
3. Conducting a suitability assessment of bidirectional TN-ITS data exchange within complete data exchange chains (data providers – data access enablers – data consumers - road end-users of data).
4. Assessing the complete end-to-end chain of TN-ITS data for vulnerabilities.

1.1. Background and Objectives of Subtask 4.2.4

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. Its primary goal is to address data priorities that fulfil the end-user needs for various mobility applications and services and ensure that up-to-date and accurate data is available to them. In the short term, TN-ITS aims to significantly support the implementation of Intelligent Speed Assistance (ISA) and the adoption of the European 'Vision Zero' strategy.[1]

Looking ahead, TN-ITS is a crucial data-sharing methodology to support automation in the long term. End-users need to be aware of and recognize the differentiating value of the TN-ITS data-sharing mechanism compared to other competitive offerings in the market. The TN-ITS framework includes a standardized data format and protocols for data exchange, ensuring compatibility and interoperability between different systems and stakeholders. It relies on a network of national and regional access points that serve as data hubs.

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 end-user. Achieving data availability, accessibility and quality is a joint effort between the public and the private sectors.

In an international EU-wide context, TN-ITS is based upon the European Committee for Standardization **(CEN)** TC 278 WG7 **standardization**, which ensures compatibility, complementarity and harmonization with other data sharing mechanisms in the entire mobility data space.

What sets TN-ITS apart is its foundation of **data trust, which** originates from the public authorities, making it the root of trust in each of the member states' road networks.

In the context of the NAPCORE project, Task 4.2.4 focuses on TN-ITS enhancements concerning the TN-ITS data-sharing chain. This task resulted from insights obtained during the

[1] https://ec.europa.eu/transport/themes/strategies/news/2019-06-19-vision-zero_en

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

CEF project TN-ITS GO (MOVE/B4/SUB/2017-63/CEF/PSA/SI2.770546) and it is a further analysis of the results obtained from the TN-ITS GO Deliverable 5.5 (Data chain requirements) and TN-ITS GO D4.1 and D4.2 (Evaluation plan and deployment of TN-ITS services).

The primary goal of Subtask 4.2.4 is to establish a trustworthy foundation and ensure the highest standards of data quality, integrity, security and sovereignty within the TN-ITS data exchange. This exchange can be bidirectional, considering the feedback loop mechanisms to enhance the quality of data. To achieve this, a technical expert team comprising NAPCORE MS and the TN-ITS ERTICO innovation platform has been assembled. This team is dedicated to conducting comprehensive research, inventorying, and assessing data trust-related items and mechanisms. The scope involves various components of the complete data exchange chains, involving data providers, analysts, publishers (National Access Points (NAP)), and consumers of data that will provide services and applications based on TN-ITS data for end-users.

Subtask 4.2.4 aims to identify the most suitable quality system for TN-ITS services based on inputs from the EU ITS Platform (EU-EIP) D4.1, TN-ITS GO, the TM2.0 (ERTICO's Innovation Platform for Traffic Management) and other NAPCORE Working Groups (WG), primarily. Furthermore, relevant developments and initiatives, such as the European Mobility Data Space (EMDS) are also closely followed. This will pave the way for defining quality levels applicable to the identified system. Furthermore, the task has and will continue to evaluate the complete end-to-end chain of TN-ITS data for vulnerabilities, classify potential attacks, and propose countermeasures. It will also recommend assessment methods and tools, such as exploring the potential for certifications, to ensure compliance and adherence to quality TN-ITS standards.

Throughout this process, close cooperation with WG3 (NAP content and accessibility) and others WGs of NAPCORE will be maintained to ensure alignment and coherence within the overall NAPCORE framework, reinforcing the collective commitment to establishing a robust and secure data-sharing infrastructure for the benefit of the Intelligent Transport Systems (ITS) community.

1.2. Scope of the report / M4.2.6

The scope of Milestone 4.2.6, in conjunction with the upcoming Milestone 4.2.7, is to strengthen the foundation for establishing a reliable and high-quality data exchange infrastructure within the TN-ITS framework. The two deliverables and their scope are explained in this section as well as in sub-section 6.2, Next Steps.

Milestone 4.2.6 aims to contribute to the evolution of TN-ITS GO, building upon the findings of the EU EIP's "SA 4.1: Determining Quality of European ITS Services", which assessed implementations within the TN-ITS GO project. It specifically focuses on the work needed to develop a comprehensive data quality assessment methodology, encompassing all aspects of the TN-ITS data chain which is a work in progress and will be presented in the subsequent draft of this deliverable. This milestone outlines concepts of trust, quality, integrity, security and sovereignty and mechanisms to enrich and assess data quality, building upon existing tools like those developed in the TN-ITS GO project along with the identification of data chain vulnerabilities and mitigation mechanisms.

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 report draws valuable insights and analysis from the EU-EIP D4.1, which focused on data quality concerning Real-Time Traffic Information (RTTI). Based on this background, and coupled with inputs from other projects, Task 4.2.4 will propose methodologies for continuous monitoring of equipment performance and availability, manual verification of entities, events, or conditions, monitoring of data completeness and latency, and monitoring of timeliness and data completeness and will be documented in deliverable M4.2.7. The report will include the findings on the potential areas for certifications (Trust and Quality), defining the necessary minimum Service Level Agreement (SLA), licenses, and digital contract elements that define the level of co-operation as well as the possibility of additional TN-ITS data and services to support the trust assessment method.

1.3. Relation to NAPCORE WG4

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

1. SubWG 4.1: DATEX II
2. SubWG 4.2: TN-ITS
3. SubWG 4.3: Multimodal data
4. SubWG 4.4: Metadata

The alignment challenge is addressed through a common task between all SWGs. This document specifically focuses on data quality aspects within the scope of the TN-ITS data chain; hence, it can be considered as important input to the WG4.

1.3.1. Association/Relationship with DATEX II

On May 24, 2023, during the Lisbon EU ITS congress, DATa EXchange between traffic and travel information centers (DATEX II) and the TN-ITS platform signed the **Declaration of Lisbon**. This declaration marks a significant milestone as the two data standards commit to merging, taking their collaboration to the next level. The action encompasses various aspects, including a joint approach to data quality and data exchange service improvements. Currently, the work primarily concentrates on harmonizing the static data layers of both standards. Furthermore, a co-operation agreement is being developed and is expected to be in place by the end of 2023, potentially encompassing a joint approach to data quality improvement.

Therefore, the scope of this document remains limited to the TN-ITS data chain itself. We anticipate that the findings and results of this task will also benefit DATEX II. Furthermore, it should be noted that tasks from the SubWG 4.1 DATEX II, such as Task 4.1.6 “Encoding and transfer”, where quality and trust concepts are considered, will need to be analyzed and assessed regularly. If possible, a collaborative effort between task technical experts should be undertaken to ensure alignment between the two standards.

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

1.4. Methodology

Dealing with this task is challenging due to the intricate interplay of data trust and quality considerations within the multi-actor, multi-functionality TN-ITS data chain. To approach this problem scientifically, a combination of desktop research, closed expert discussion and workshop feedback has been devised. Furthermore, the methodology is conducted in two distinct phases.

The first phase involves extensive desktop research on the topics of trust, quality, integrity, security and sovereignty, both generally and within the transportation domain in particular. This helps establish a better understanding and formulate suitable definitions to achieve a common understanding of these terms. The efforts conducted within the framework of the EU EIP and TN-ITS GO projects have laid the essential groundwork for the methodology, enabling the utilization of the invaluable expertise possessed by the project participants. A thorough evaluation of the TN-ITS data chain was carried out to highlight the potential vulnerabilities and challenges at each data chain phase, as illustrated in Figure 1.

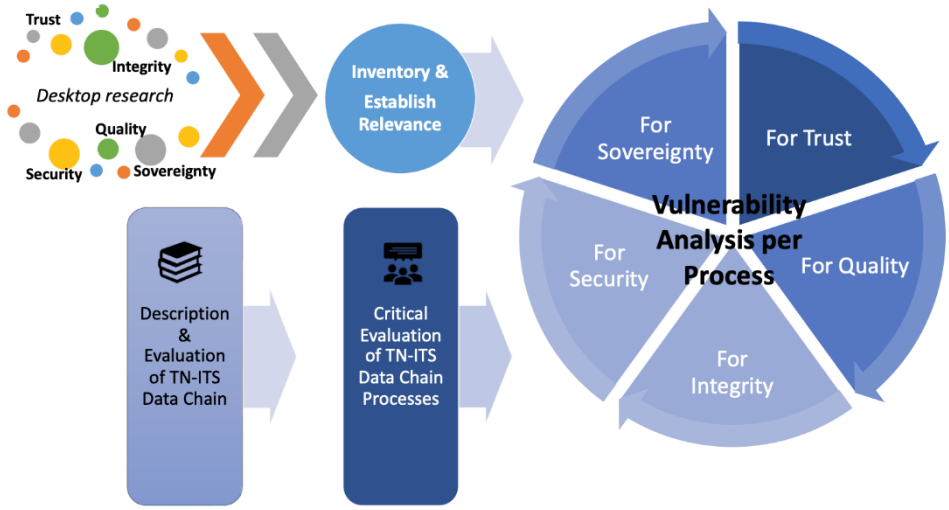

Figure 1 – Task 4.2.4 Methodology: Phase 1

The second phase of the methodology involves the critical assessment of potential vulnerabilities and mitigation measures, relevant inputs from NAPCORE and other projects. During the last quarter of 2023 and the first half of 2024, analysis will be conducted in expert meetings or focus groups and the findings shared and validated in workshops to identify data chain improvements and propose TN-ITS quality assessment framework and quality enrichment and evaluation tools, as illustrated in Figure 2.

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

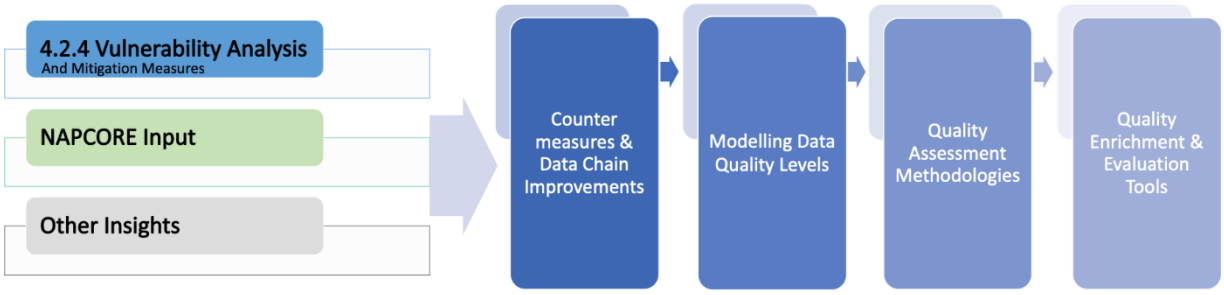

Figure 2 – Task 4.2.4 Methodology: Phase 2

The expected relevant NAPCORE inputs are listed in subsection 2.2.4. It should be noted that as work progress, some NAPCORE project findings will be more relevant to this work than others. The findings of Phase 2 will be documented in M4.2.7, which will be published in Dec 2024. A detailed description of future work is presented in section 6.2 of this document.

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

2. Definitions and references

2.1. Data sharing related quality aspects

To establish a common understanding, this section covers the definition of key terms, such as data trust, quality, integrity, security and sovereignty. It should be noted that these terms are discussed within the domain of ITS and pertain specifically to the TN-ITS data ecosystem.

2.1.1. Trust

According to H. L. J. Ting et al. (2021), digital trust plays a crucial role in the context of digital agents exchanging services and information, which is relevant to the TN-ITS exchange. The paper "On Trust and Trust Modeling for the Future Fully-Connected Digital World"[2], defines digital trust as a measurable belief and/or confidence that is built over time from past experiences and encompasses an expectation of value for the future. Trust is quantified based on evidence and past interactions. Meanwhile, there are several properties to be considered such as:

- Subjective Trust Levels: Trust levels vary between individuals, with some being stricter and others more lenient. Trust values and decision boundaries should reflect individual preferences rather than a universal standard.
- Context-Dependent Trust Levels: Trust levels also vary depending on the context. Different digital environments may attract entities with different intentions, and each interaction within a specific context may differ from others.
- Dynamic Trust: Trust tends to diminish over time as existing knowledge becomes outdated. Trust models should account for the decay of trust with time without overcompensating.
- Transitive Trust: Trust can be transferable. When a trusted individual recommends someone, trust in the recommender implies trust in the recommendation. The extent of trust transfer depends on the digital environment and individual agent.
- Asymmetric Trust: Trust formed between a truster and a trustee is directed, meaning trust in one direction does not imply trust in the other. Asymmetry can exist in trust relationships, particularly when there is an imbalance of authority, however, certified authorities are likely more trustworthy.
- Easy to Lose but Hard to Gain: Trust can be easily lost and challenging to regain. Caution is exercised in digital environments to ensure security, leading agents to prefer interacting with trusted, familiar entities. Trust is forfeited relatively quickly when betrayed.
- Pervasive Nature of Trust: Trust is a fundamental prerequisite for any interaction, both in social and digital communities. Trust is pervasive in digital communities, and agents rely on trust to function effectively in the digital world.

Data trust refers to the confidence and reliability placed in the quality, integrity, and security of data. It involves the belief that data is accurate, trustworthy, and can be used to make informed

[2] H. L. J. Ting et al.: On Trust and Trust Modeling for Future Fully-Connected Digital World

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

decisions. Data trust is built through mechanisms such as data governance, transparency, accreditation, data quality assessment, and adherence to ethical and legal standards.

Trust in the context of TN-ITS refers to the confidence and belief that stakeholders have in the reliability, credibility, and integrity of the map data exchanged through the system. It encompasses the faith placed in data sources, the security and privacy of the data, the transparency of processes, and the overall dependability of the information provided. Trust is built through measures such as data source verification, transparency, accreditation, security, and user feedback, fostering confidence in the accuracy and trustworthiness of TN-ITS data.

Trust accumulates from past mutual experiences in the data sharing relationship between a data provider and a data user. It largely impacts the stakeholders' expected value for the future.

TN-ITS functions as a data standard and an exchange mechanism between the authority and the service provider. This authoritative aspect should be 'the root of trust' for this data and service, making it a genuine differentiator from other data sources and services provided by private partners, for instance. Their trust can only be based upon their 'brand recognition' as authorities.

2.1.1.1. Detailing the 'trust aspect'

The following figure gives an overview of the trust elements[3] that this document will consider:

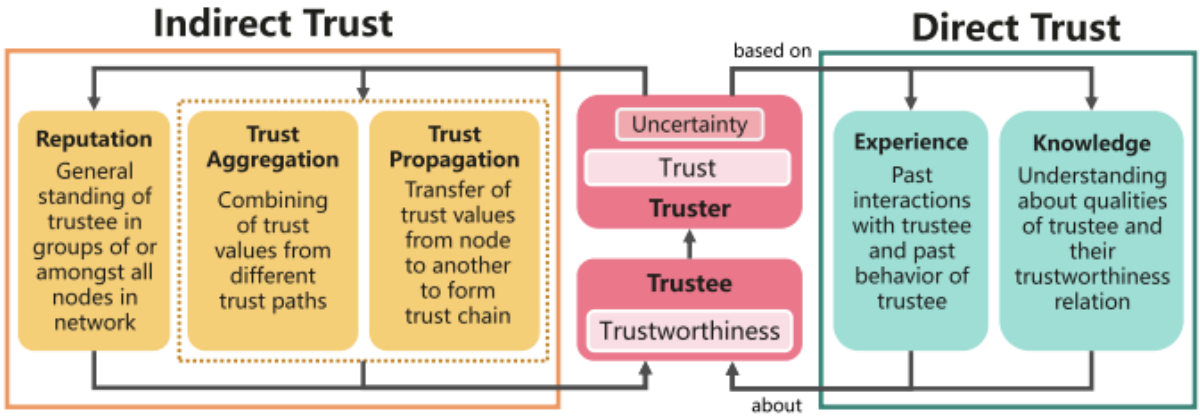

Figure 3 – The Trust Elements - H. L. J. Ting et al. (2021)

2.1.1.2. Trust-related aspects

The following table gives more insights into the elements that impact the trustworthiness of data and the TN-ITS service. This catalogue was the result of a survey amongst the active members of the NAPCORE task SWG4.2.4.

[3] H. L. J. Ting et al.: On Trust and Trust Modeling for Future Fully-Connected Digital World

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

Trust categories	Trust attributes	Trust categories	Trust attributes
Root of trust	What is it and what is the basis?	Data quality	Proper documentation
	What is the definition?		Syntax correctness of data
	What is the scope?		Semantic correctness
	Subjects to trust: data, production process, publishing network		Check with physical reality, data validation
Brand recognition	Credibility		Restrictions for data production
	Market recognition		Accuracy
	Competitive aspects		Accessibility
	Who is the data supplier (trust level of authority or public domain)		Availability
	Reputation		Network coverage
	Responsiveness (follow-up questions etc)		Frequency of updates
ICT aspects	Cybersecurity (e.g. SEML)		Completeness
	Quality ICT standards (ITIL)		Comprehensiveness
	Authorisations		Expectations of end-user/service provider
	Authentication		Dis-ambiguity and consistency
	API/exchange mechanism		Validity, freshness and accuracy (time stamp)
	Integrity handling		Mandatory updating of old data, being old depends on the data set
	Sovereignty handling	Regulatory aspects	Mandatory publishing
	Back-up for data loss		Mandatory usage
	Automation of data checks and verifications		Responsibility for quality: data producer or service provider,

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

Trust categories	Trust attributes	Trust categories	Trust attributes
			user ultimately responsible for data usage
Service quality	Availability of Service level Agreements	Organisation aspects	ISO 900x
	Need versus availability (feedback loop)	Price/Cost	Price: "I pay a lot hence, I can trust/expect"
Compliance	Authoritative seal (Label0)	Audibility	How can we audit it?
	Testing requirements		Supporting rules/regulations
Standards adherence	CEN	Sustainability	GDPR
	ISO		Sovereignty
	NAP		Fairness

Table 1 – Elements that Impact the Trustworthiness of Data and the Service

Table 1, as mentioned earlier, is the result of feedback from some members of Task 4.2.4 where they presented their concerns about what should be taken into consideration in M4.2.6 and the future M4.2.7 related to TN-ITS data trust. Therefore, throughout this report, some of these trust requirements will be inventoried and/or analyzed for Milestone 4.2.7 to present more efficient and comprehensive results regarding the TN-ITS data assessment methodology and the creation of a coherent and systematic evaluation system.

2.1.2. Quality

The EU-EIP project recognizes the paramount importance of data quality in the domain of ITS. Within the EU-EIP framework, data quality plays a critical role in ensuring the accuracy, reliability, and usability of the data exchanged and utilized for various ITS applications.

From the view of the EU-EIP, data quality refers to the level of accuracy, completeness, consistency, timeliness, and relevance of data used in ITS. It represents the fitness for use of data and encompasses various dimensions, such as accuracy, completeness, consistency, validity, reliability, and relevancy. Ensuring high data quality is crucial for maintaining reliable and effective ITS operations.

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

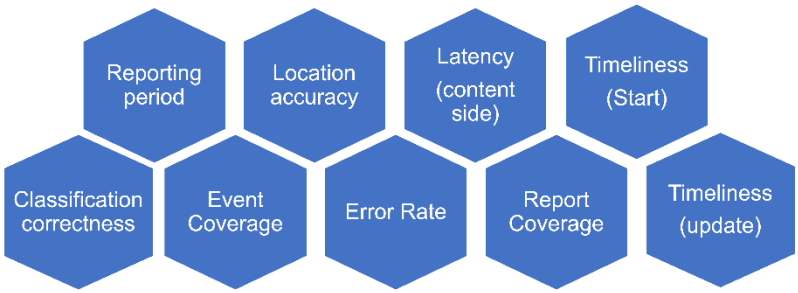

Figure 4 – EU-EIP Data Quality Parameters

2.1.3. Integrity

Data integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle. It ensures that data is not corrupted, altered, or compromised and that it remains intact, trustworthy and authentic, throughout the entire lifecycle, including data collection, transmission, storage, and processing. Data integrity is critical for making informed decisions and maintaining the trustworthiness of ITS applications. Data integrity is maintained through mechanisms such as data validation, error detection and correction, access controls, and backup and recovery processes[4].

2.1.4. Security

Data security involves protecting data from unauthorized access, disclosure, alteration, or destruction. It encompasses measures and safeguards to ensure the confidentiality, integrity, and availability of data[5]. Data security practices include encryption, access controls, authentication, secure storage, network security, and compliance with data protection regulations. Data security in ITS encompasses safeguarding sensitive information related to traffic management, vehicle communications, and personal data[6]. Since TN-ITS primarily focuses on enhancing road safety, improving traffic efficiency, and providing drivers with more reliable navigation guidance, secure data transfer is a requisite.

2.1.5. Sovereignty

The term data sovereignty is a widely used concept in data management, particularly in the context of data protection and cross-border data transfers. It is a legal and policy concept that refers to the jurisdictional control and regulatory authority that a country or organization has over the data collected, processed, or stored within its borders [7]. It encompasses the rights and control that a country or organization has over the data and determines who can access, manage,

[4] Chen, C., Li, R., & Lin, W. (2017). Enhancing Data Integrity for Vehicular Networks. IEEE Transactions on Intelligent Transportation Systems, 18(4), 870-880. DOI: 10.1109/TITS.2016.2592722

[5] Huang, Y., et al. (2019). Securing Vehicular Networks: Challenges, Countermeasures, and Future Directions. IEEE Communications Surveys & Tutorials, 21(3), 2489-2522. DOI: 10.1109/COMST.2019.2895360

[6] Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security (4th ed.). Cengage Learning.

[7] Esayas, S., & Mungai, C. (2021). Data Sovereignty: Definitions, Models, and Practices. In Trust and Security in Data Science (pp. 167-192). Springer. DOI: 10.1007/978-3-030-78984-2_7

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

and use the data. Data sovereignty is closely related to data privacy and data protection laws[8]. Data sovereignty influences data sharing, data protection, and data governance practices in ITS applications.

Data sovereignty is a crucial aspect within the TN-ITS eco-system as the data source is usually a road authority and ensuring the sovereignty of this data is crucial for a proper and legally binding implementation of ISA.

2.2. Relevant standards, regulations and projects/initiatives

2.2.1. Standards

The initiatives demonstrate the efforts being made to enhance trust and quality in the field of ITS. They address various aspects such as data integrity, security, cooperative communication, and standardization to ensure reliable and high-quality services for transportation systems.

ISO 37123:
ISO 37123 is an international standard that addresses the measurement and management of sustainable cities and communities. It includes indicators related to the quality of transport infrastructure, accessibility, road safety, and traffic management, which contribute to building trust and ensuring high-quality ITS services.

DATEX II (Data Exchange for Traffic Information):
DATEX II is an XML-based standard for exchanging traffic-related information. It provides a common data model and message format for the exchange of traffic data, including traffic events, road conditions, and travel-related information. TN-ITS leverages DATEX II for the exchange of location-referenced map data.

ISO 14825 (Traffic and Travel Information - Location Referencing for Traffic Management and Traffic-Related Information):
ISO 14825 standardizes location referencing methods and mechanisms for traffic and travel information. It defines the principles and requirements for location referencing in traffic management and related applications. TN-ITS aligns with ISO 14825 for location referencing of traffic data.

ISO 19112 (Geographic Information - Spatial Referencing by Coordinates):
ISO 19112 specifies principles and methods for spatial referencing using coordinates. It provides guidelines for expressing and handling coordinates to describe geographic locations. TN-ITS can utilize ISO 19112 for spatial referencing of map data.

CEN/TC 278 (Intelligent transport systems):
CEN/TC 278 emphasizes data quality and trust in ITS standards. It underscores the need for accurate, reliable data to ensure safe and efficient transportation. The committee highlights data integrity, consistency, and timeliness. Establishing trust in data sources, sharing, and processing

[8] Strasser, T., & Ozdemir, D. (2017). Data Sovereignty in Smart Cities. Journal of Urban Technology, 24(4), 77-95. DOI: 10.1080/10630732.2017.1371711

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

is vital for effective ITS implementation. Adhering to data protection regulations is stressed, promoting privacy and security. CEN/TC 278's standards address data quality assurance mechanisms, fostering trust among stakeholders. Harmonized data standards and validation procedures are crucial for consistent, dependable ITS operation.

CEN TC287 WG7:
CEN/TC 287 is the European counterpart of ISO/TC 211 (Geographic information/Geomatics) and is not to be confused with CEN/TC 278 (Intelligent transport systems), which is the counterpart of ISO/TC 204 (Intelligent transport systems). CEN is the European Committee for Standardization, and ISO is the International Organization for Standardization. The work in these international standards bodies is organised in Technical Committees (TCs). The ongoing standardisation activity of TN-ITS concerns the work to bring the TN-ITS specification for a spatial road data exchange framework to the level of a CEN Technical Specification. This work is carried out jointly by TN-ITS WG 2 (Specifications and Standardisation) and CEN/TC 278/WG 7 (ITS spatial data).

2.2.2. Regulations / Directives

EU ITS Directive (Directive 2010/40/EU):
The ITS Directive aims to establish the framework for the deployment of ITS within the EU. While it focuses on interoperability and standardization of data exchange for improving mobility and transport services, it indirectly encourages data quality through data accuracy and harmonization.

EU Regulation on the Provision of EU-wide Real-time Traffic Information Services (2015/962):
This regulation aims to improve the availability and quality of traffic information to enhance mobility and reduce congestion. While it doesn't directly address data quality, providing accurate and reliable real-time traffic data is crucial to achieving the intended objectives.

EU Regulation on a Framework for the free flow of non-personal Data in the European Union (2018/1807):
The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at the Union level (‘codes of conduct’), to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards. The regulation includes a mandate for the Member States to develop approaches to certification schemes related to quality management.

EU Regulation on a list of specific high-value datasets and the arrangements for their publication and re-use (2023/138):
The regulation is set up under the Open Data Directive, which defines six categories of such high-value datasets: geospatial, earth observation and environment, meteorological, statistics, companies, and mobility. The regulation states that quality of service criteria should be shared with the data.

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

Implementing act on a list of High-Value Datasets (HVD):
The Open Data Directive (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information) outlines the requirements for MS to identify and publish lists of high-value datasets, which should be made available for use in fields such as transportation. These high-value datasets are expected to have significant economic and societal impact, and their availability for reuse can foster innovation and data-driven solutions. For data that could have relevance in future mobility usage, datasets judged to be High value are GPS data, 3D mapping, maps (national and local, cadastres/land registry, land usage, terrain form, postcodes, topography, and city 3D models, subject to current or future data exchange by TN-ITS.

General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679:
The GDPR is a comprehensive regulation that addresses data protection and privacy for individuals within the EU. Although it does not explicitly focus on data quality or the ITS domain, it emphasizes the importance of accurate and up-to-date data. Article 5 of the GDPR outlines the principles of data processing, including the requirement that personal data must be accurate and kept current. Furthermore, it mentions data accuracy, data minimization and accountability.

Open Data Directive - Directive (EU) 2019/1024:
The Open Data Directive aims to promote the availability and reuse of public sector data across the EU. While it does not explicitly address data quality, the directive encourages public sector bodies to publish data in machine-readable formats and to provide metadata that includes information on the data's quality and accuracy.

European Data Quality Guidelines:
While not a regulation, the European Data Quality Guidelines provide recommendations and best practices for data quality management in the context of European Statistical System (ESS) data. These guidelines aim to enhance the quality of statistical data, including open data, and ensure its coherence and comparability across EU member states.

2.2.3. Projects/initiatives (non-exhaustive)

Projects listed in this section demonstrate ongoing efforts to address trust and data quality in the ITS domain. They aim to develop frameworks, methodologies, and tools that ensure the reliability, accuracy, and integrity of data in various ITS applications, contributing to the trustworthy deployment of connected and autonomous vehicles and improved traffic management services.

Traffic Management 2.0 (TM 2.0):
TM 2.0 is an initiative that aims to improve the trustworthiness and 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. This initiative generates an important contribution towards TN-ITS data chain quality improvement. Related to ‘data trust’, TM2.0 produces ‘levels of co-operation’ between public and private partners. TN-ITS can use such a model, as the level of co-operation is always the basis of the level of trust. If the data is the result of intense co-operation between the service

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

provider and the authority, then it can be 'more' trusted. M4.2.6 and M4.2.7 will further develop this model by defining the necessary minimum Service Level Agreement (SLA), licenses, and digital contract elements that define the level of co-operation.

SENSOR Interface Specification (SENSORIS):
Sensoris is an open group of actors from the global vehicle industry, map and data providers, sensors manufacturers and telecom operators who joined forces under this innovation platform. Driven by the common vision, the actors define an appropriate interface for exchanging information between the in-vehicle sensors and a dedicated (OEM) cloud and the interface from the cloud toward the service provider. The availability of this type of data can play an important role in the 'feedback loop' concept (see further).

Data for Road Safety (DFRS):
DFRS provides a scalable solution where any industry partner in the transportation, mobility and traffic data domain and public authorities can join and start using to exchange safety-related traffic data and information. This raw data is processed towards 7 'security warning information, that is available to further communicate with end-users. The nature of this service requires accuracy in data. The data itself can play a role in the 'feedback loop principle'.
DFRS is an ERTICO innovation platform, that digitalizes a scalable solution where any industry partner in the transportation, mobility and traffic data domain and public authorities can join and start using it to exchange safety related traffic data and information.

CONnected CORridor for Driving Automation (CONCORDA☺
CONCORDA is a H2020 European project that aims to establish trust in automated driving by ensuring data quality, cybersecurity, and privacy. It focuses on developing a trustworthy and secure data exchange framework for connected and automated vehicles.

FLOURISH:
FLOURISH is a UK-based project that focuses on trust and acceptance of connected and autonomous vehicles (CAVs). It addresses the challenge of data quality by developing methods to validate and ensure the accuracy of CAV sensor data, enabling trustworthy decision-making in autonomous vehicles.

CoEXist:
CoEXist is an EU-funded project that focuses on enabling the coexistence of automated and conventional vehicles in urban areas. It addresses trust and data quality by developing methods for validating and ensuring the accuracy of data from different sensors and data sources used by connected and automated vehicles.

SENTINEL:
SENTINEL is an EU-funded project that focuses on trust, security, and data quality in the context of cooperative and connected automated mobility. It aims to develop a comprehensive security framework for cooperative ITS applications, including methods for ensuring data integrity and trustworthiness.
Traveller Information Services Association (TISA):
TISA is an international industry association that promotes the development and standardization of traffic and travel information services. TISA focuses on ensuring the quality and trustworthiness of traffic information, including data exchange protocols, data quality

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

assessment, and harmonization of data formats. TISA focuses on data exchange services between the service provider and the end -user.

TISA handles the standard TPEG, a standardization initiative that focuses on the reliable and efficient exchange of traffic and travel information. TPEG aims to enhance the quality and accuracy of information by defining data formats, protocols, and coding schemes for various ITS applications, including navigation systems and traffic information services.

Navigation Data Standard (NDS Live)
NDS.Live is the new generation of the worldwide standard for map data in the automotive eco-system. It caters to the transitions of navigation from pure offline to hybrid/online, enables cloud connected dynamic data, addresses the growth of map data in size and needs to update only what needs updating over a data connection, as well as further improved support for autonomous driving. NDS live focuses on data exchange services between the service provider and the end -user.

PrepDspace4mobility
PrepDspace4mobility lays the foundation for a secured and controlled way of pooling and sharing mobility data across Europe. It contributes to the development of the common European mobility data space by mapping existing data ecosystems, identifying gaps and overlaps within, and proposing common building blocks and governance frameworks found in existing data space architectures

TN-ITS Go
TN-ITS GO was a Programme Support Action (PSA) (2018-2021) for the implementation and facilitation of seamless spatial data exchange which are essential for the deployment of ITS applications, to give time to 13 Member States to plan and implement carefully their ITS spatial data supply chain strategy right from the source (police decision, road maintenance,), all the way to the open TN-ITS interface and into the map database of the end user. The project created insights into the TN-ITS data chain quality aspects, e.g. TN-ITS Go D5.5 (Data chain requirements) and TN-ITS GO D4.1 and D4.2 (Evaluation plan and deployment of TN-ITS services). The topic of trust and data quality was also addressed in D2.3 Data store maintenance and TN-ITS roll out, addressing the ICT environments and processes in place to operate the service.

Open AutoDrive Forum (OADF)
TN-ITS is since June 2019 official member of the OADF. The OADF is a cross-domain platform driving standardizations around autonomous driving. Members of the OADF are the consortia ADASIS, NDS, SENSORIS, SIP-ADUS, TISA and TN-ITS.

The goals and missions of the OADF are to act as an open discussion platform for cross domain topics around autonomous driving that require cooperation throughout the industry. It generates globally applicable, state-of-the-art solution possibilities as further input for standardization in organized bodies and connects local authorities and the global industry to streamline future development efforts. The platform also presents the latest developments and achievements toward a connected world of autonomous cars.

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

2.2.4. Reference to other NAPCORE activities

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	**Task 2.2**: Definition of requirements concerning data standards, reference profiles, metadata and support tools	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.
	Task 2.3: NAP Architecture	A set of functional and technical requirements to harmonize the functions and interfaces of NAPs.
WG3	**Task 3.2**: European NAPs data quality	Subtask 3.2.1 – Quality Framework where quality criteria and levels of service of the EU-EIP were considered.
		Subtask 3.2.2 – Guidance & best-practices for quality assessment
		Subtask 3.2.3 – Quality certification for NAP datasets
	Task 3.3: Data access and reuse	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.
SWG4.1	**Task 4.1.5:** Modelling and Usability	This 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
	Task 4.1.6: Encoding & Transfer	
SWG4.4	**Task 4.4.2.4**: Draft Specification	Work Item Accompanying Guideline regarding metadata quality criteria
WG5	**Task 5.3:** Quality and evaluation criteria	Focusing on the requirements of compliance assessment, (common) quality and evaluation criteria will be defined, to be used by national bodies/competent authorities. This task will be carried out in close cooperation with WG3, referring to quality criteria identified for data and services as published via the National Access Points.

Table 2 – Quality and Trust Tasks from the NAPCORE 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

3. State of the art know-how

This section will report on the advancements and insights that have been made in the domain of data trust and quality within the ITS domain that are relevant to the TN-ITS. They will serve as input for further work, leading to the follow-up deliverable (M4.2.7) of this work task.

3.1. TN-ITS GO

In TN-ITS GO the following relevant information can be found in the following deliverables.

3.1.1. D2.3 Data store maintenance and TN-ITS roll-out

The following text is from TN-ITS GO - Deliverable D2.3, chapter 1. This deliverable addresses the ICT environments and processes in place to operate the service.

i. Generic TN-ITS data store architectures

This task identified two major process steps that member states need to perform to enable their TN-ITS service. One major step is about 'data availability' and the second one is about 'data accessibility'. The data availability relates to the 'data store", while data accessibility relates to the 'TN-ITS service roll-out'.

As an example, the architecture of Cyprus is taken to illustrate the implementation of TN-ITS data store architecture.

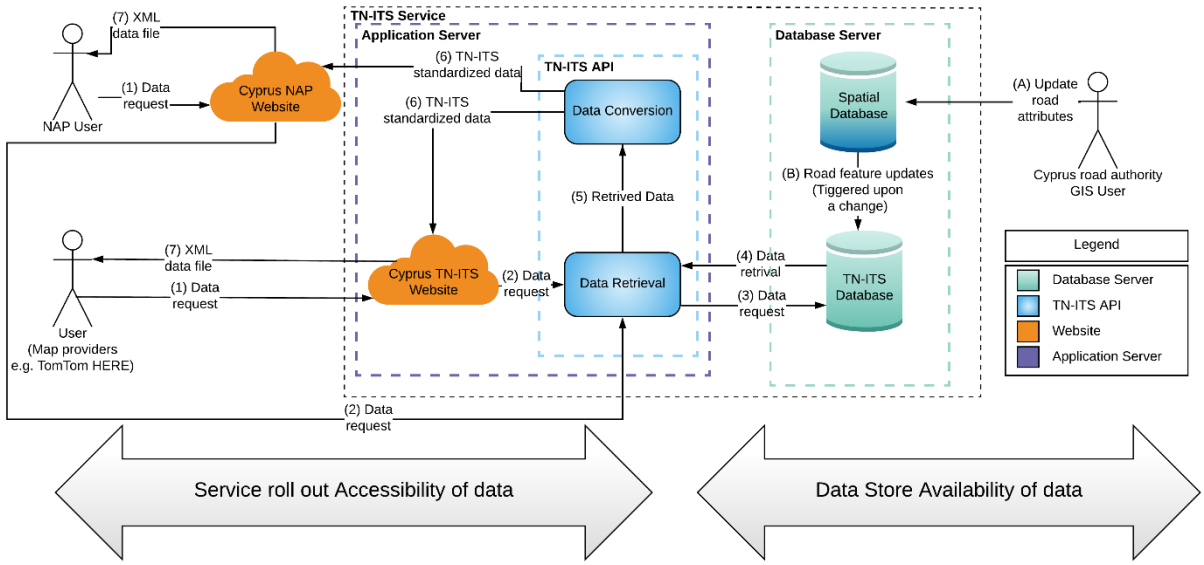

Figure 5 - TN-ITS Data Store Architecture –Cyprus Example

ii. Life cycles

The data store considers two different types of life cycles. One life cycle deals with the TN-ITS product life cycle, while the second life cycle deals with the data itself. The following figure illustrates both life cycles.

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

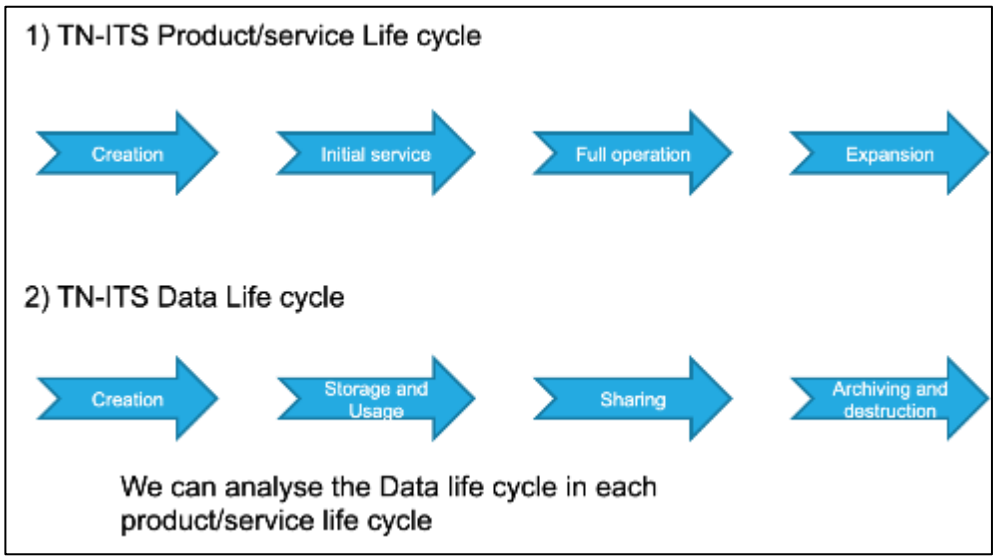

Figure 6 - TN-ITS Types of Life Cycles in the Data Store

iii. Data Store procedures (Data availability part)

It is the viewpoint that each MS authority needs to establish the necessary internal procedures for the maintenance of the data life cycle in each established technical elements to perform the TN-ITS service but are still in the definition and writing phases of the related procedures to maintain and grow the service which might be impacted by ongoing initiatives such as the DATEX II and TN-ITS merger.

The following table illustrates a potential cataloguing of the necessary procedures and can explain their status.

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

	Creation	Initial service	Full operation	Expansion
Creation	*Procedures for gatheringvarious applied data sources and how you maintain them, Own production of data, …)*			
Storage & Usage		*Procedures for Maintaining quality of data (Methods can include: monitoring of equipment and performance, Maintaining statistics, manual verification, testing, sampling, surveys by users, feedback loop reporting,*	*Procedures for back-ups handling*	
Sharing		*Procedures for Data transformation - Data Validation, Re-formatting, Consistency of data, …*	*Procedures for Maintaining integrity of data, including Cyber security aspects, root of trust handling, …*	
Archiving & destruction	*Procedures for archiving and destruction of various applied data sources)*			

Table 3 – TN-ITS Data Store Procedures

iv. Service roll-out (Accessibility of data)

The following table illustrates a guideline to member states to report on the procedures for 'service roll out', along the life cycle of the TN-ITS product/ service.

Creation	Initial service	Full operation	Expansion
Initial Procedures for transferring Map update data atributes	*Procedures for NAP handling or any other type of transfers*	*Procedures for trust –integrity handling along the delivery channel*	
		SLA's	
		Licenses	

Table 4 – TN-ITS Service Roll-out Procedures

3.1.2. D4.1 and D4.2 (Evaluation plan and deployment of TN-ITS services)

The following text is from TN-ITS GO - Deliverable D4.2, chapter 3.

i. Evaluations related to the access and performance of the Web-services

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 ***access*** and the ***performance*** of the web-services will be evaluated based on principles discussed earlier in the TN-ITS taskforce for SLA. The ***availability*** is measured and documented by the provider over a period (bd) to determine the up-time. ***Incident management*** is evaluated on support hours, response time and resolution time.

Three service quality levels are identified, related to the obtained evaluation results: **Basic**, **Elite** and **Ultimate**. These levels of services are described in the table below:

TN-ITS Service Levels **Support services**	**Basic** **(low)**	**Elite** **(medium)**	**Ultimate** **(high)**
Service Availability (over a period):	90%	96%	99,9%
Incident management – support hours	Office hours	Office hours	24x7
Incident management – Initial response time	1 day	4 hours	1 hour
Incident management – Target resolution time	Reasonable effort	1 day	4 hours

Table 5 – TN-ITS Service Quality Levels

ii. Evaluations related to the 'structure of TN-ITS data' (protocol)

The evaluating partner will check the correctness of the data format and compliance of the XML files provided in the TN-ITS Service Pilot.

iii. Evaluations related to the 'location referencing' (accuracy checks)

The accuracy of the location of the provided updates and report on the overall correctness will be evaluated.

iv. Data Content check vs. other sources (Features and Attributes)

Quality checks of the data content will be performed similarly by Väylä, TomTom and HERE and reported in a standard template.

v. Evaluations on the Feedback loop, (Statistics on published data)

The TN-ITS service with Feedback loop data to the service of Väylä is provided and planned individually by TomTom and Here.

3.1.3. TN-ITS GO D5.5 (Data chain requirements)

The following text is from TN-ITS GO - Deliverable D5.5, chapter 3.

i. Data Chain Requirements

The table below gives an inventory of the top-level requirements that can be imposed on the different functions, identified in the data chain:

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

Stakeholder	Data chain function	Aspect	Requirement
	Data (regulation data…)	Trustable	Credibility, reliability, or reputation
		Secure	Access rights, modification/read /write /personnel code, etc.
		Authenticity & Authentication	Authority by regulation?
		Quality	Correctness
			Completeness or comprehensiveness
			Consistency, coherence, or clarity
			Accuracy
			Timeliness or latency (freshness)
			Validity or reasonableness
		Compliance to specification	CEN based formats
		Documented	
		Performance	Geo coverage representation
			Road attribute coverage
			Accessibility
			Availability
			Update frequency
		Secure	Protection against attacks
		Access rights	
		Quality aspects	
		Data integrity	
		Unique identifier	Visual progress monitor
		Time management: beginlifespanversion, endlifespanversion	Visual progress monitor
	MS ICT infrastructure	Information Technology Infrastructure Library	
	MS TN-ITS infrastructure	Service compliance according to TN-ITS API	

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

Stakeholder	Data chain function	Aspect	Requirement
	Automation tools data/Capturing population	Accuracy	Geolocation, validity time, Time stamp
		Correctness	
		Authorised personnel	
Communication	Comms channel		Integrity
		HTTPS	Encryption
Service/Map provider		Authorised personnel	
		Secure environment?	
		Performance	

Table 6 – TN-ITS Inventory of the Data Chain Requirements from TN-ITS GO D5.5

ii. Methodologies to fulfil the requirements

The following table complements the previous table with the insights generated by the project partners on potential tools and methodologies that could be used to fulfil data chain requirements, imposed at each function.

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

Stakeholder	Data chain function	Aspect	Requirement	Actual status TN-ITS GO	Potential tools and methodologies as solutions for the requirements	Details	Potential further actions	Comments	Advice Recommendations
Authority									
	Data (regulation data...)	Trustable	credibility, reliability, or reputation		Watermark/logo//based on all other aspects below.	Creation of a watermark within the TN-ITS forum, Deploying the watermark is MS -should be on feature level- marketing	To be worked out in NAPCORE		
		Secure	Access rights, modifiction/read /write /personnel code/...		Local MS to organise the security aspects and service level agrrements with subcontracts	What is the role of the NAP, Secure data piping is necessary/Cfr MDM Germany (security certificates/Who is using the data// NAP needs registration tools and authenticity tools	Should we provide guidelines?-Are their tools ?	License is open data , but data users needs registration-subcription based, authentication needed	Advice not to be encrypted data because of size ,(latency/too complicated
		Authenticity & Authentication	Authority by regulation?			See above			
		Quality	Correctness	Syntax, Symantics & fit with the reality is lacking	Feedback loop--correctness on syntax (today)--Manual process (Validation tool)-	The fit with reality is lacking ? --SENSORIS ?-payd service by the service provider-collaborative tool for citizens (Like Waze,...)	Correctness should be checked at creation level		
			Completeness or comprehensiveness	We lack the overal regulation (METR?)		See above			
			Consistency, coherence, or clarity			See above			
			Accuracy	Geolocation , validity, the right info		See above			
			Timeliness or latency (freshness)		Improve the procedure throughput time to go from the initial regulation towards publishing the related digital dataset	Provide guidelines, metadata description, last changed timestamp/ Operational excellence label		To be worked out and be concsious on time scale and resources.-- benchmarks on aggregated level? (Austria that creates regulation and immedieatly the data related to it	What tools are availble//We do have finding and inspring examples--example UK
			Validity or reasonableness			Validy time stamp is available in TN-ITS Go (occasonally)- imposed -	To be worked out in NAPCORE		
		Compliance to specification	CEN based formats		Feedback loop	Validation tools (HERE-TomTOm) available			
		Documented			MUST				
		Performance	Geo coverage representation	Scope is Ten T	% of network	Revision of RTTI delegated act says only primary roads			
			Road attribute coverage		% of the list of manadatoryattributes	RTTI delegated act revision			
			Accessibility		NAP				
			Availability						
			Update frequency		Version mgt of spec-- Related to CEN and the commissionm				

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

Stakeholder	Data chain function	Aspect	Requirement	Actual status TN-ITS GO	Potential tools and methodologies as solutions for the requirements	Details	Potential further actions	Comments	Advice Recommendations
Authority (continued)	MS database	Secure	protection against attacks		Should be easy for data users/Should be uniform across EU	Best practice guidance inpires by the MS--state of the art			
		Access rights							
		Quality aspects							
		Data integrity							
		Unique identifier ?	cfr Visual progress monitor						
		Time management : beginLifeSpanVersion, endLifeSpanVersion	cfr Visual progress monitor						
Authority (continued)	MS ICT infra	itil?							
	MS TN-ITS infra	Service compliance according TN-ITS API			Feedback loop				
	Automation tools data/Capturing population	Accuracy	Geolocation, validity time, Time stamp						
		Correctness							
		Authorised personnel							
Comms	Comms channel		Integrity						
		https? File download	encryption		Checksum/data catalogue /Automated end to end system				
Service provider		Authorised personnel ?							
		Secure environment?							
		Perormance.when is the map ready?			Service level agreement	Benchmarking? OEMS?			

Table 7: TN-ITS tools and methodologies to be used to fulfil the data chain requirements

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

3.2. TM2.0 model

This traffic management model is based on the level of co-operation between the data provider and the service provider. TM2.0 is a ('r)evolution from TM1.0 where road operators and service providers do not co-operate and develop their own separate information and control loops. TM2.0 resulted in integrated information and control loops since it is based on the following principles:

i. Collaboration and trust
ii. Alignment of information to drivers and consistency
iii. Co-opetition: understanding among stakeholders on interests and needs

Resulting in integrated information and control loops.

This model is still evolving. The actual status is illustrated by the following figure.

(Abbreviations: PA: public authority; SP: service provider; RO: road operators; TMC: traffic management center)

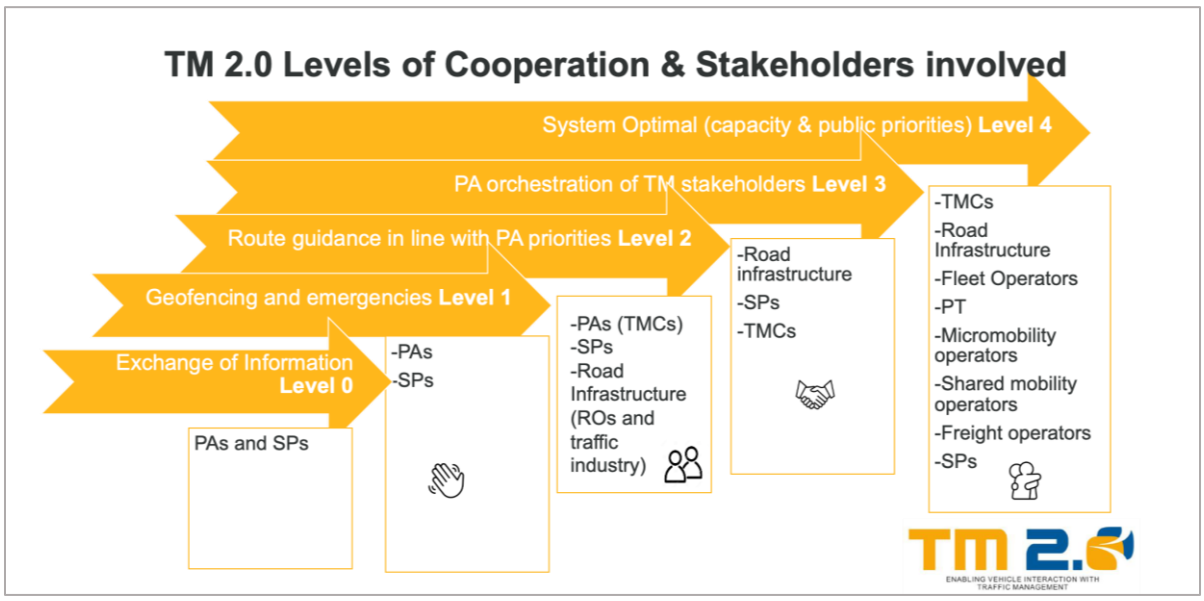

Figure 7 – TM 2.0 Model Levels of Co-operation

This initiative significantly contributes to the improvement of TN-ITS data chain quality. Related to 'data trust', TM2.0 produces 'levels of co-operation' between public and private partners. TN-ITS can use such a model, as the level of co-operation is always the basis of the level of trust. Data resulting from intense cooperation between the service provider and the authority can be considered more trustworthy.

M4.26 and M4.2.7 intends to further develop this model by defining the necessary minimum SLA, licenses and digital contract elements that define the level of co-operation.

3.3. EU-EIP

The EU-EIP has published extensive analyses on data quality tools and methodologies. The project findings form the basis for further technical analysis during the SWG4.2 NAPCORE project tasks.

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

3.3.1. EU-EIP Quality Levels / Requirements Model

EU EIP sub-activity 4.1, presents a chapter focusing on the "Optimum Quality". This task examines the level of quality of traffic information and its impact on user perception and decision-making. The approach aims to analyse the optimum quality levels for selected quality criteria and provide recommendations to all TN-ITS actors (e.g. EU MS, road authorities and others TN-ITS standard community) on quality improvement options.

The quality of information in traffic services plays a crucial role in how frequently users utilize the service and how it affects their decision-making. Low-quality information leads to ineffective decision-making, diminishing the societal benefits and incurring costs in terms of traffic safety and traffic flow. Improving information quality typically comes at a cost, and research suggests that there exists an "optimum quality level[9]" beyond which further improvements do not produce significant benefits.

To quantitatively analyse the optimum quality of ITS services, data on production costs, quality levels achieved with investments, and estimates of societal benefits are required. However, the available quantitative quality information is limited and difficult to compare due to its focus on specific aspects or impacts, without considering the relevance of different quality parameters.

Quality requirements refer to the minimum quality levels that individual TN-ITS data and services should achieve. These requirements determine the baseline at which the Quality Criteria must be met to fulfil specific quality expectations. The study provided expert judgments on the "optimum quality level" or "target quality level" (the level organizations should strive for) for different quality criteria based on the EU EIP Quality Package levels: **Basic (*)**, **Enhanced (**)**, and **Advanced (***)**.

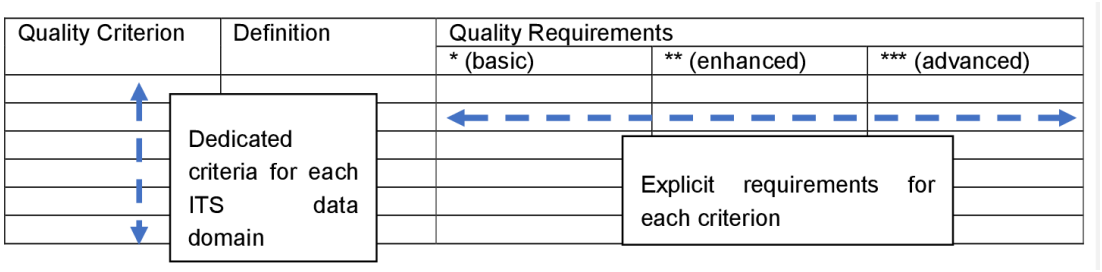

Figure 8 - EU EIP Quality Packages Suggested Approach[10]: Tabular Structure for describing Quality Criteria and Quality Requirements

i. **Basic level (*)** - The most crucial Quality Requirements are the ones in the basic level. All services based in TN-ITS must meet this level, as providing a lower quality service would likely result in negligible or even negative user benefits.
ii. **Enhanced level (**)** - Involves improving the dataset and services beyond the basic level. This includes resolving any errors, filling in missing information, and standardizing data formats. Additionally, enhanced data quality may involve data enrichment, where supplementary data from reliable sources is integrated to provide

[9] https://www.its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/Quality%20Frameworks/EU%20EIP%20SA%204%201%20%20Optimum%20Quality%20-%20Final%20Report%20-%20Feb%202021.pdf

[10] Review of EU EIP Quality Frameworks for NAPCORE WG3 by Peter Lubrich (Federal Highway Research Institute, DE)

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

more comprehensive insights. The enhanced level of data quality enables more advanced analytics, better decision-making, and a higher level of confidence in the data.

iii. **Advanced level (***)** - Represents the highest level of data excellence achievable. At this level, data is not only accurate, complete, and consistent but also highly reliable, timely, and aligned with specific business needs. Advanced data quality incorporates sophisticated data governance practices, data profiling, and ongoing monitoring to maintain data integrity and ensure compliance with industry standards and regulations. Organizations can confidently utilize data for complex analytics, predictive modelling and strategic decision-making, contributing to their overall success and competitive advantage.

The future selection of TN-ITS criteria for the "**Data evaluation tools for the *TN-ITS standard trust assessment method and quality system***" to be developed in the next 4.2.7 milestone will also be based on the well-established EU-EIP Level of Service and Quality Criteria[11], which will serve as a solid foundation for evaluating the methodologies.

[11] https://www.its-platform.eu/activities/activity-4-harmonization-cluster/sa-4-1-determining-quality-of-european-its-sevices/

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

	Definition of Quality Criteria for RTTI and SRTI		Applicable for	
			Event Information	Status-Oriented Information
Level of Service	**Geographical coverage**	Percentage of the road network covered by the (content provision) service	X	X
	Availability	Percentage of the time the (content provision) service is available	X	X
Level of Quality	**Timeliness (start)**	The time between the occurrence of an event and the acceptance of the event	X	-
	Reporting period	The time interval for refreshing / updating the status reports	-	X
	Timeliness (update)	The time between the end or (safety) relevant change of condition and the acceptance of this change	X	-
		The average age of the sensor data used in the most recent reporting period	-	X
	Latency (content side)	The time between the acceptance of the event or its end or (safety) relevant change of condition and the moment the information is provided by the content access point	X	-
		The time between the calculation of the reporting data and the moment the information is provided by the content access point	-	X
	Location accuracy	The relative accuracy of the referenced location for the published event with respect to the actual location of the actual event	X	-
	Classification correctness	100% minus the percentage of the published events which are known to be not correct, concerning actual occurrence of this event type / class	X	-
	Error Rate	Percentage of published status reports which show excessive deviations of a reported quantity (e.g. speed or travel time) versus the actual value or are otherwise determined as erroneous	-	X
	Event coverage	Percentage of the events which are known to be correctly detected and published by type / class, time and location (i.e. detection rate)	X	-
	Report coverage	The percentage of reporting locations for which a status report is received in any given reporting period	-	X

Table 8 - EU-EIP Level-of-Service and Level-of-Quality Criteria for RTTI and SRTI

In the TN-ITS data chain, the level of service measures the overall performance of a system or service at a specific time, while data quality criteria involve specific standards (requirements) used to measure that performance. Both aspects, level of service and data quality criteria, are vital for assessing user experience and system functionality in the realm of mobility.

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

4. TN-ITS data chain

This chapter provides an overview of the TN-ITS data chain, highlights the data chain stages, identifies its potential vulnerabilities and possible mitigations, identifies the stakeholders involved and the data sources.

4.1. History of the data chain: ROSATTE and eMaPS

The ROSATTE project, initiated in 2008, aimed to address the difficulties faced by map and service providers in obtaining updated road data from various European authoritative sources, each with their data formats. The primary goal of the project was to assist road authorities in effectively and efficiently making these changes available to applications that benefit the public.

Funded by the EC (2008-2010, DG INFSO/DG Connect), the ROSATTE innovation project focused on establishing collaboration between public and private entities to create and maintain "safety attributes" in map databases. The project developed standardized procedures to facilitate access, exchange, and upkeep of road safety spatial data across Europe from public sources. It aimed to enable the aggregation and updating of European-wide safety data at various levels—national, regional, and local. The project also evaluated the technical and organizational feasibility of implementing this infrastructure.

The project consortium consisted of road authorities from Norway, Sweden, France, Bavaria, and Flanders, as well as road operators like ASFA and TfL. Private organizations such as Tele Atlas and NAVTEQ participated as map makers and service providers. The figure below illustrates the defined and piloted Data Chain, depicting the roles, data flow, and data processes involved.

The technical specifications developed within ROSATTE served as the foundation for subsequent standardization efforts by CEN TC278. These efforts culminated in the publication of CEN Technical Specification 17268 in December 2018.

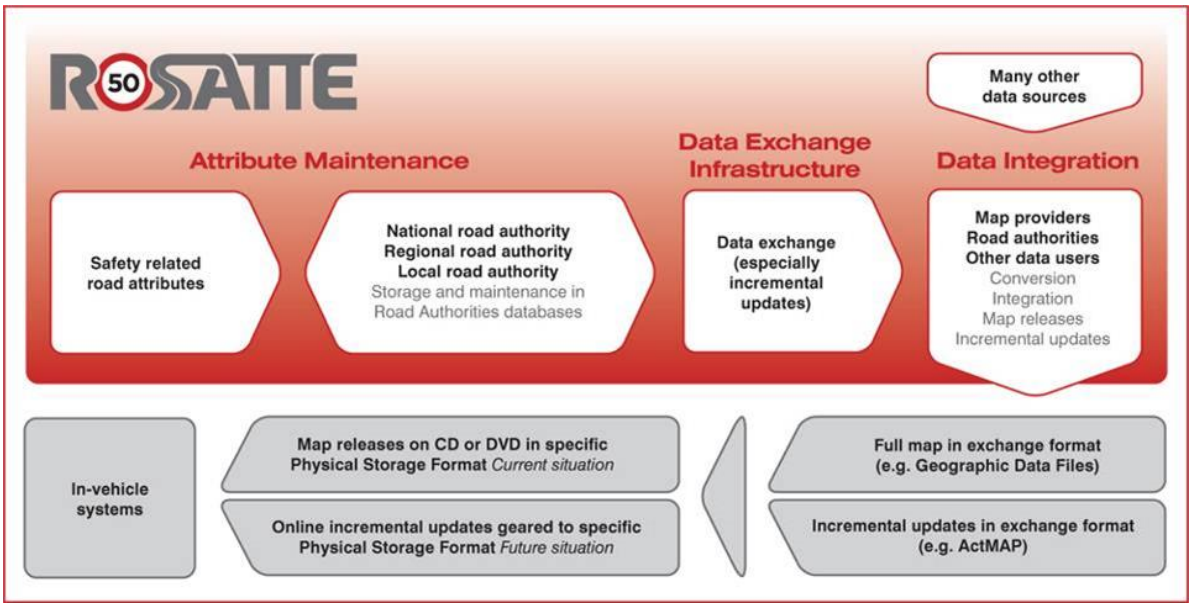

Figure 9 – The ROSATTE Project – Data Chain Pilot

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

Following the completion of the ROSATTE project, the eMaPS project (FP7, eSafety Digital Maps Public Private Partnership Support, 2011-2012) was initiated as a continuation. Its purpose was to establish an independent implementation platform called the "ROSATTE Implementation Platform." This platform aimed to facilitate the implementation of actions 1.2 "Collection and provision of road data" and 1.3 "Accurate Public Data for Digital Maps" outlined in the ITS Directive. The Norwegian Public Road Administration (NPRA) led the eMaPS project, and it retained the original team of experts from the ROSATTE project to provide support and guidance to newcomers from the public road sector.

Eventually, the ROSATTE Implementation Platform underwent a name change and became known as the "TN-ITS platform."

4.2. History and future of the data chain: reference to: TN-ITS Go

TN-ITS GO, the successor to the EU EIP project Sub-activity 4.7 for pilot TN-ITS implementation, aimed to advance the TN-ITS concept and enhance the engagement of MS in TN-ITS activities. To achieve this, the strategy was to establish implementation activities in more EU MS. Building on the achievements of the Transportation Pilot's success, new pilot TN-ITS services were initiated in five additional EU MS as part of the EU EIP project's sub-project (Sub-activity 4.7). This sub-project received funding through the 2014 call of the Multi-Annual Programme of CEF Transport.

The TN-ITS sub-project began in January 2016 and concluded in mid-2017 (formal deadline: 31 December 2017). Finland, Flanders/Belgium, the United Kingdom, Ireland, and France participated as the involved MS. The testing of their respective data chains and providing advice were undertaken by the ITS map providers HERE and TomTom, with TN-ITS (via ERTICO-ITS Europe) acting as the Sub-activity coordinator. Close collaboration with the INSPIRE community (JRC, ELF project) allowed for the incorporation of their expertise and the extension of the experience gained during the Transportation Pilot.

The TN-ITS Go project commenced in January 2018, with an expanded scope encompassing nine more states preparing for their TN-ITS service implementations. These countries include The Netherlands, Hungary, Cyprus, Lithuania, Portugal, Slovenia, Spain, Estonia, and Greece. The ultimate aim of TN-ITS Go was to foster wider adoption of TN-ITS across Europe, driving harmonization and cooperation among MS to create a seamless and effective cross-border ITS network. By fostering active involvement and collaboration, TN-ITS Go achieved safer, more efficient, and sustainable transportation systems across the continent.

The TN-ITS data chain has undergone a significant evolution during the TN-ITS GO project. The following image illustrates the data chain that was defined in the TN-ITS GO 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

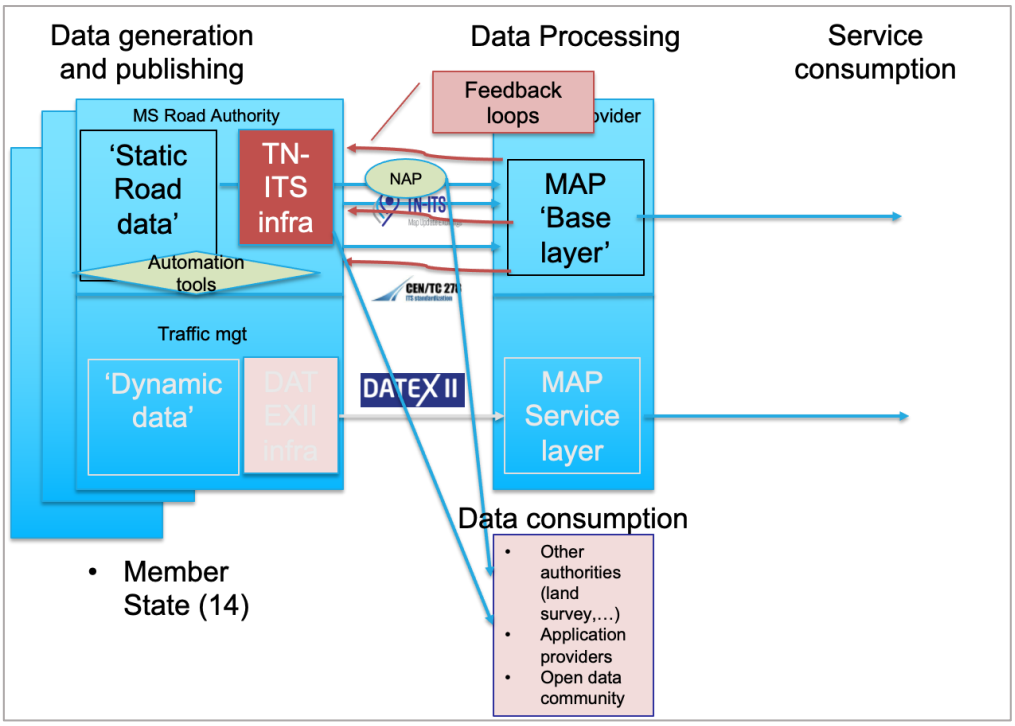

Figure 10 – TN-ITS Data Chain at the End of TN-ITS GO Project 12/2021

In the workshop of 01/12/2021 (D5.5 of TN-ITS GO) the following future data-chain was identified:

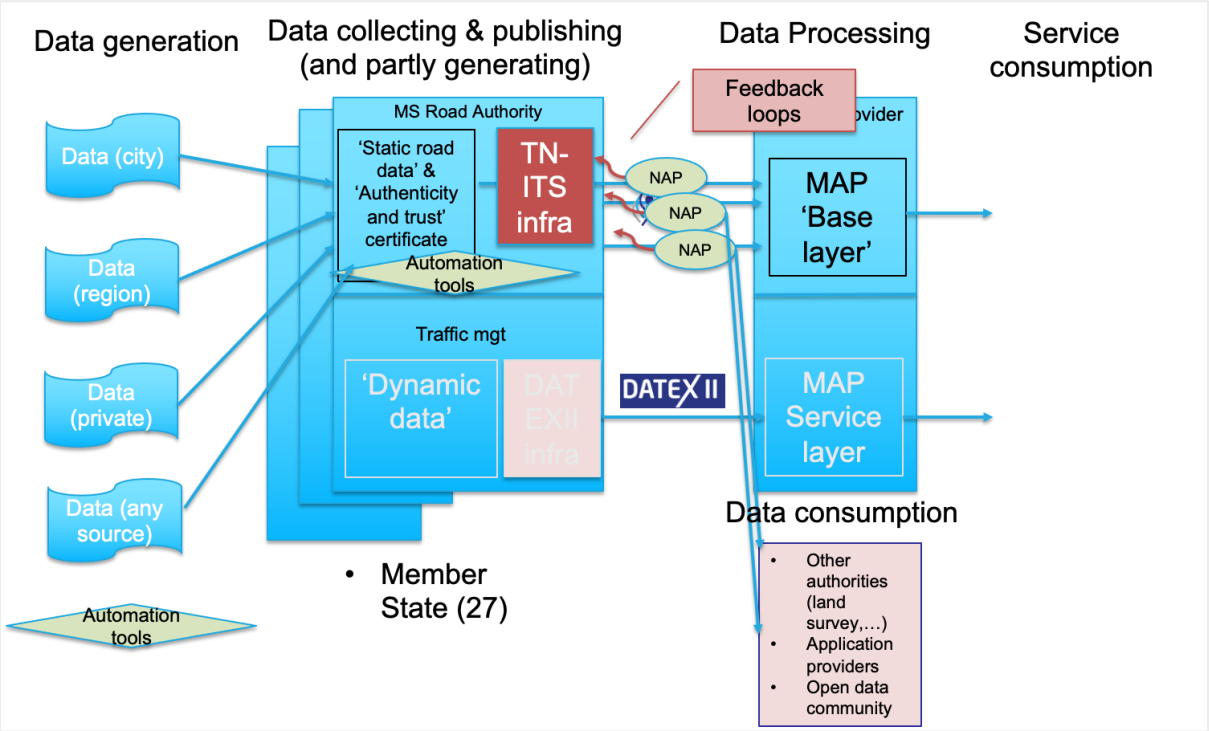

Figure 11 – TN-ITS Data Chain Identification after 12/2021

This data chain details the roles of additional stakeholders for data generation and details the role of the road authorities: Data collecting, publishing and partly generating themselves. The illustration does not mention the role of the NAP specifically, but it can be identified as the 'distributor' role. The TN-ITS data chain is further extended and updated in the next chapter.

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

4.3. Reference TN-ITS data chain and vulnerabilities

The reference TN-ITS data chain based on Figure 12 is presented in this section. The TN-ITS data chain encompasses multiple stages which are integral to the seamless data flow. Each stage plays a vital role in ensuring the accuracy, reliability, and effective utilization of data from production until the usage process.

An introductory overview of the five stages involved in the TN-ITS data chain is illustrated in the figure below. The stages are Data Collection, Data Processing, Data Exchange, Data Integration and Data Usage.

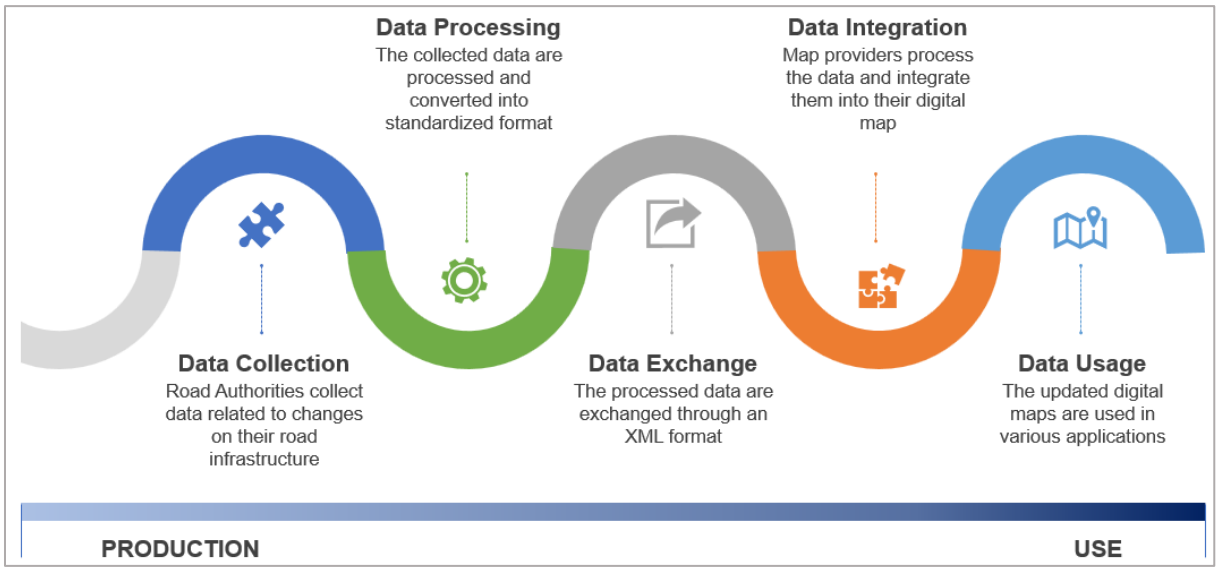

Figure 12 – Reference TN-ITS data chain (George Christou, KIOS Center of Excellence, ITS Congress Lisbon 2023)

While the TN-ITS data chain offers immense potential for improving road safety and optimizing traffic management, each stage is susceptible to vulnerabilities. Here, we will present the five data chain stages and delve into the distinct vulnerabilities that may emerge within each of these stages. This exploration encompasses potential obstacles, risks, and points of failure. Understanding these vulnerabilities is essential for developing robust mitigation strategies and ensuring the integrity and reliability of the TN-ITS data chain.

i. Data collection

The Data Collection stage plays a crucial role in acquiring map-related data from diverse sources, including road authorities and the automotive industry (see the list of all TN-ITS data providers in the subchapter "TN-ITS Stakeholders"). It involves gathering data from sensors, cameras, connected vehicles and also includes data regarding changes in road infrastructure and road attributes.

However, this stage is susceptible to multiple ***vulnerabilities***, such as incorrect data input stemming from circumstances like data tampering (also result of data manipulation attacks), sensor inaccuracies, inadequate coverage, and data provenance issues.

ii. Data Processing

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 services such as TN-ITS.

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

Still, ***vulnerabilities*** can arise due to incorrect standards or data values. Issues such as algorithmic biases, erroneous data transformations, inadequate data anonymization techniques, and computational resource limitations can result in the use of incorrect data values.

iii. Data Exchange

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 or/and through the MS NAPs.

However, ***vulnerabilities*** in this stage can occur due to malicious data injection through unauthorized access resulting in privacy breaches targeting the confidentiality of the data and data leakage caused by cyberattacks such as Distributed Denial of Service (DDoS) attacks or malware infections. Lack of standardization and incomplete or inconsistent metadata also pose significant risks to the integrity of the exchanged data.

iv. Data Integration

Data Integration is the stage where map providers process and integrate data into their digital maps, focusing on merging unlike datasets from multiple sources into a cohesive and consistent format.

Vulnerabilities in this stage primarily revolve around the possibility of incorporating wrong data into the maps. These vulnerabilities can arise due to data compatibility issues, conflicting data schemas, poor data mapping techniques, and semantic heterogeneity. Intentional actions can also be applied at this stage, such as data inconsistency attacks, in which conflicts are intentionally introduced into the data chain to increase its resistance to such issues.

v. Data Usage

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.

However, ***vulnerabilities*** at this stage can lead to the display of false or wrong information. Challenges include data misinterpretation, improper utilization of context, biased decision-making, and a lack of transparency in data-driven processes. Malicious entities can also display false information/data.

4.4. A Circular TN-ITS Data Chain

The previous discussion leads to the following circular data chain model where a new stage is included, the Feedback Loop. It is illustrated in the figure below along with the description of the newly added stage.

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

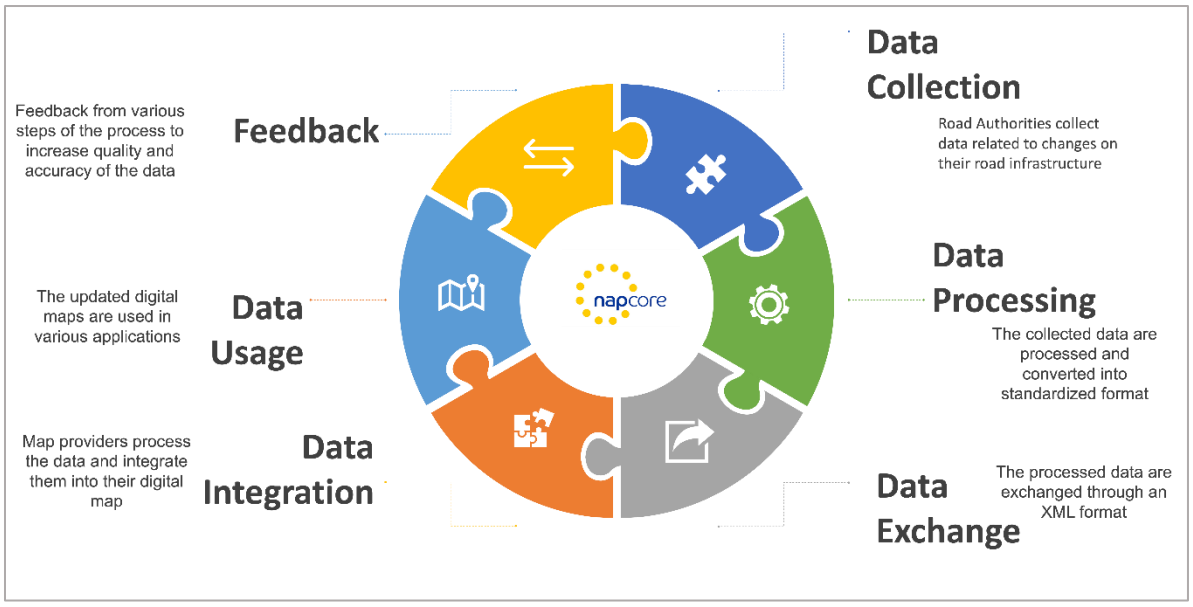

Figure 13 – The Up-to-Date Circular TN-ITS data chain (George Christou, KIOS Center of Excellence, ITS Congress Lisbon 2023)

vi. Feedback loop

The feedback loop emerges as an indispensable mechanism that plays a key role in fortifying the TN-ITS data chain against most of the potential vulnerabilities mentioned above. By establishing a continuous cycle of communication, evaluation and improvement, the feedback loop serves as a proactive measure to identify, address, and mitigate vulnerabilities throughout the five steps of the data chain mentioned previously.

To ensure bidirectional TN-ITS data exchange within the complete data exchange chains, it is imperative to first understand the multiple data chain feedback possibilities among the TN-ITS actors. The Feedback Loop can follow two different sequences:

i. Following the sequence *provider* > *publisher (e.g. publishing through the NAP)* > *analyst* > *consumers* of the data chain, the feedback loop allows providers of data to make available valuable insights and updates to the analyst and publisher. This information enables the analyst and publisher to enhance data collection methodologies, improve data processing techniques, and ensure data accuracy, thereby fostering a continuous improvement process.

ii. Following the sequence *consumers of data* > *analyst* > *providers*, the data consumers can provide feedback to the analyst, enabling them to fine-tune data processing methodologies and data integration techniques to better suit the needs of data end-users. The analyst can then convey relevant insights to the provider, closing the loop and ensuring a seamless flow of information between all stakeholders.

It is also important to mention that within the feedback loop, we distinguish between:

- The **syntax** feedback loop: Feedback is provided on the accuracy of data coding with the established standard.

- The **semantic** feedback loop: For data quality, a major topic is the ‘semantic’ feedback loop. (= a context driven check between physical and digital realities). The loop is partly

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

in place (maybe not deployed everywhere), using e.g. SENSORIS methods, but it only goes from OEM to the service provider. There is not yet a standard for the 'Service to Public Authorities' interface (TN-ITS already defined a methodology for 'syntax feedback= check on coding accuracy against the standard).

To evaluate the vulnerabilities within the TN-ITS data chain comprehensively, a holistic end-to-end analysis is necessary. This analysis should encompass all stages, examining potential risks such as data manipulation, cyberattacks, privacy breaches, data inconsistencies, and the impact of malicious entities. Thorough vulnerability assessments, risk analysis frameworks, and continuous monitoring mechanisms should be employed to ensure the trustworthiness of the TN-ITS data chain.

4.5. TN-ITS Data Chain Stakeholders

The TN-ITS data chain involves various stakeholders, each playing a crucial role in successfully implementing and operating the TN-ITS data chain. These stakeholders can be broadly categorized into three main groups: data providers, data access enablers, and data consumers. These categorized stakeholders form a collaborative ecosystem within the TN-ITS data chain. Their collective efforts ensure the availability and usability of accurate and up-to-date data, contributing to the overall success and effectiveness of the TN-ITS data chain and the broader ITS domain.

It should be noted that an attempt was made to adopt a list of stakeholders that generally represent the MS. However, it must be understood, given the different realities between MS, that the same list does not comprehensively represent the specific reality of a particular MS.
This section provides an overview of the stakeholders in each category.

i. **Data Providers and/or Data owners** – These stakeholders are entities responsible for generating and supplying accurate and reliable data related to traffic and navigation. In some cases, data owners might be a different entity than the data provider while in some other cases data providers and data owners compromise the same entity. The role of data providers and data owners concerning data sovereignty within the TN-ITS data chain will be further evaluated in task 4.2.4. They play a fundamental role in ensuring that up-to-date and relevant information is available for consumption by other stakeholders. The following are some key stakeholders in the data provider category:
    - National Mapping Agencies: National mapping agencies contribute geospatial data, including road network geometry, traffic regulations, administrative boundaries, etc.
    - Road Authorities (National, Regional and Local level): Road authorities are responsible for providing data on road infrastructure, such as speed limits, road signs, road attributes, real-time data, etc.
    - Automotive Industry: Automotive manufacturers and suppliers provide data on vehicle-specific attributes, such as dimensions, weight limits, and advanced driver assistance systems (ADAS) requirements, etc.
    - Concessionaires (i.e. private road operators).
    - Other map providers (e.g. Google, Open Street Map…
    - Crowd sourcing
    - IoT devices

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

ii. **Data Access Enablers** – Entities that facilitate the exchange and distribution of data within the TN-ITS data chain. They ensure that data providers can effectively share their information with data consumers. The following are some key stakeholders in the data access enabler category:

- National Access Points (NAPs): NAPs act as intermediaries between data providers and consumers, providing a centralized access point for data exchange or as a weblinks platform, seamlessly connecting users to valuable datasets that might reside in separate sources.
- Standardization Bodies: Standardization bodies, such as CEN and ISO, define and maintain the technical standards and protocols necessary for data exchange in the TN-ITS data chain.
- Open Data Platforms: Data Aggregator platforms that collect data from various sources with unified metadata. Open Data platform aims to enable the government and private sectors to exchange and share open data with consumers, start-ups and academia to improve public services, support decision-making, and promote economic growth.
- Private Data Marketplaces: One potential future enabler in the data access ecosystem for the TN-ITS data chain is the concept of private data marketplaces. A private data marketplace would function as a platform where data providers and consumers can exchange data in a controlled and regulated environment. However, it is essential to acknowledge that as of the current context, there are existing legal and commercial barriers that need to be addressed to realize the full potential of private data marketplaces in the TN-ITS data chain.

iii. **Data Consumers** – Stakeholders that utilize the data available in the TN-ITS data chain to provide services and applications for end-users. They rely on the accurate and timely information provided by data providers and access enablers to deliver value-added services. The following are some key stakeholders in the data consumer category:

- Map and Service Providers: Map and service providers are crucial stakeholders in the TN-ITS data chain as they rely on real-time traffic information to enhance the accuracy and relevance of their navigation and mapping solutions. By integrating TN-ITS data, these providers can offer up-to-date and dynamic routing guidance, ensuring drivers are informed about the latest traffic conditions, congestion, and road closures.
- Land Surveying and Cadastral: For this purpose, TN-ITS data is of immense value in accurately capturing and recording changes in road networks. By incorporating real-time traffic information, surveying professionals can maintain precise records of road attributes, ensuring land records remain updated and reflective of current road conditions.
- App Developer (Start-up): Start-up app developers can greatly benefit from accessing TN-ITS data, as it opens opportunities for innovation and the creation of new applications. By incorporating real-time traffic information into their apps, they can offer unique and valuable services to end-users, contributing to a more diverse and competitive app ecosystem.
- Data Brokers: Data brokers act as intermediaries in the TN-ITS data chain, facilitating the exchange of traffic-related information between data providers and consumers. Their role is crucial in ensuring a smooth flow of data and optimizing data availability and usability for various industries and applications.
- Open Data: The concept of open data fosters transparency and collaboration. Open data initiatives that utilize TN-ITS data can empower researchers, academics and other projects to access traffic information freely. This

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

accessibility can lead to the development of innovative solutions, informed policy-making, and a deeper understanding of traffic patterns.

- Regulatory Bodies and Public Authorities (Internal Consuming): These are key consumers of TN-ITS data, using it to monitor and manage traffic, make data-driven decisions, and implement policies to enhance road safety and efficiency. Real-time traffic information empowers these entities to respond proactively to changing traffic conditions and address congestion and potential hazards promptly.
- Vehicle Manufacturers and TIER1 Suppliers: Automotive industries, including vehicle manufacturers and TIER1 suppliers, can leverage TN-ITS data to enhance in-car navigation systems and advanced driver-assistance features. By incorporating real-time traffic information, they can improve route planning, optimize driving experiences, and promote safer, more efficient journeys for drivers.

iv. **Road End-Users**: Road end-users are the culmination of the previous list of data consumers, including drivers, cyclists, and pedestrians, who are the ultimate beneficiaries of the TN-ITS data chain. They rely on the accurate and timely information provided by data consumers to make informed decisions and enhance their travel experience.

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, ETSC, VIAS), consumer organizations (EURO NCAP), 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.

4.6. Examples of TN-ITS Data Source

The purpose of this subchapter is to identify some examples of the data sources for the TN-ITS data chain. Understanding the origins of data is crucial for ensuring the accuracy and reliability of the information used in the TN-ITS system.
Currently, the data within the TN-ITS data chain primarily comes from regulatory bodies, which deliver trust in the information provided. These regulatory bodies play a significant role in collecting and maintaining the data required for the system's functionality.
The following sources are a few examples employed to populate the TN-ITS databases:

- Apps: The Movin' app (FL-BE) and the Hungarian application on smart mobile devices are key contributors to the data chain, offering essential data related to transportation.
- Hand-filled database and digitalization of maps: User interface within the road authority which serves as a platform for inputting data into the TN-ITS system when regulations change, or new information is to be added.
- People reporting information: Citizens play an essential role in reporting information mismatches, such as incorrect speed limits on the street or other discrepancies. Their feedback helps to improve the accuracy and reliability of the TN-ITS data.

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

- Buying of commercial maps if possible: Commercial maps are acquired to enrich the data sources when feasible. These maps contribute additional location-specific information to enhance the TN-ITS database.
- Future Possibilities: Apart from the existing data sources, future scenarios for expanding the TN-ITS data chain include the integration of various technologies, such as Sensors (e.g. real-time data, road conditions and other relevant parameters), IoT devices and ID devices (Identification devices to track vehicles).

4.7. TN-ITS role in a Mobility Data Space

The definition of a mobility data space is still ongoing. The TN-ITS view is that data space is an ecosystem of stakeholders (partners) where data exchange happens. It is a value chain where data is exchanged from one partner to the other, increasing the value of the data.

In this context, maybe 'Mobility Data Space' is synonymous with 'data chain'. If we consider TN-ITS as one part of a mobility data space, then we can refer to the next figure explaining the elementary functionalities that should be present in the space.

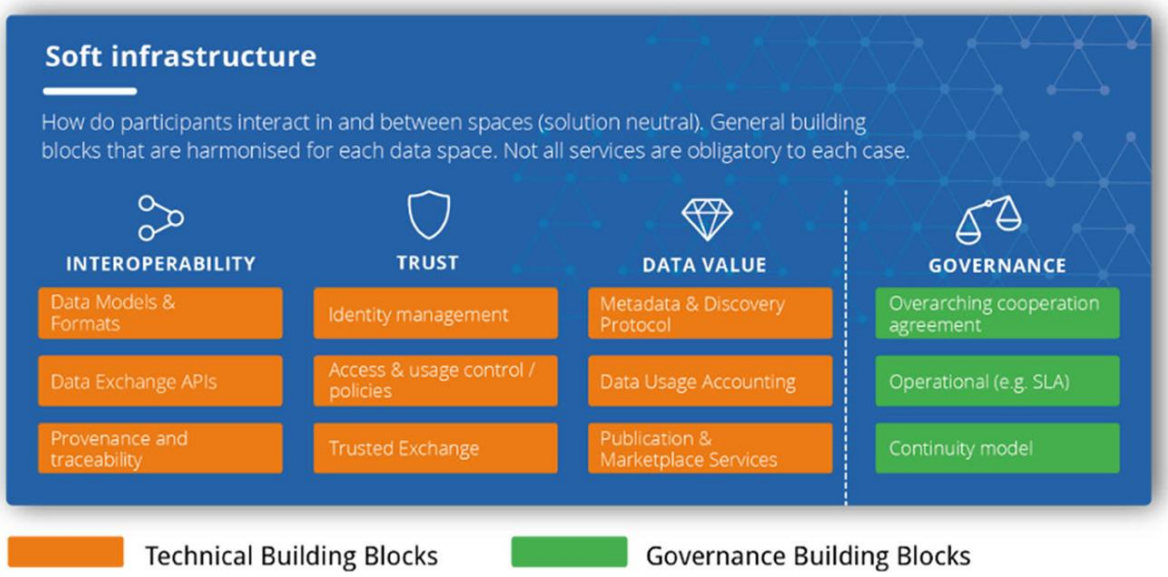

Figure 14 – Building blocks for data spaces (©2021, International Data Spaces Association)

The Dataspace Connector (DSC) is an open-source software for sovereign data exchange. Even after the data has been exchanged, the data provider remains in control of what happens to the data. The connector function explains how data should be shared from one node (data provider) to the other node (data consumer) in the chain. The next figure shows the necessary functionalities that go along with the connector.

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

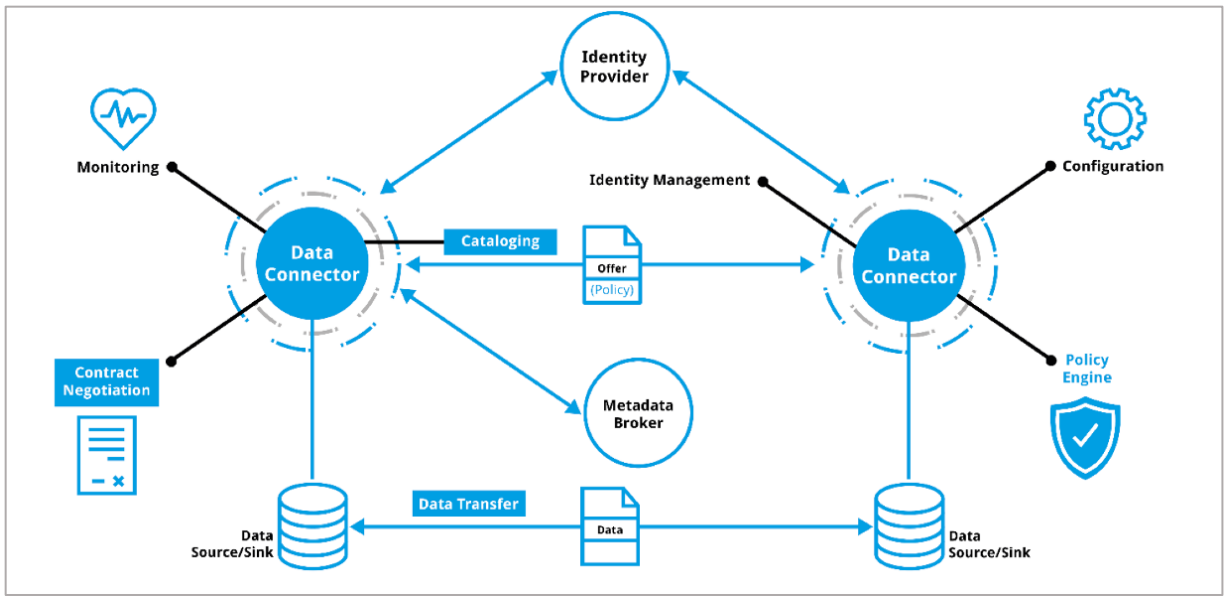

Figure 15 – An example diagram of data connectors (MDS) [12]

In Milestone 4.2.7 we will analyse in depth how these mobility data space requirements are fulfilled in TN-ITS and how we can improve the data chain (or Mobility Data Space).

[12] Designing data spaces, Springer, https://link.springer.com/content/pdf/10.1007/978-3-030-93975-5.pdf?pdf=button

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

5. Inventory of requirements to improve trust, quality, integrity, sovereignty and security of data

In this chapter, the intention is to carefully analyse the vulnerabilities present within the TN-ITS data chain and identify potential attacks that could compromise the integrity and reliability of the system. The process of mitigating these vulnerabilities and potential attacks holds the key to the creation of an assessment method made specifically for the TN-ITS data chain and the development of enhanced data evaluation tools (both tasks to be implemented in Milestone 4.2.7).

Building upon the insights gained from previous chapters that explored the TN-ITS data chain and researched the status of data quality, the focus now shifts to a comprehensive examination of the weaknesses of the TN-ITS data chain.

5.1. Inventory of vulnerabilities and potential data attacks

In the following table, the main and secondary vulnerabilities, and potential attacks of the TN-ITS data chain, from the previous chapter, are listed.

Data Chain Stage	Main Vulnerability	Secondary Vulnerabilities
Collection	Incorrect data input	➢ Data tampering (data manipulation attacks) ➢ Sensor inaccuracies ➢ Inadequate coverage ➢ Data provenance
Processing	Incorrect standards or data values	➢ Algorithmic biases ➢ Erroneous data transformations ➢ Inadequate data anonymization techniques ➢ Computational resource limitations
Exchange	Malicious Data Injection	➢ Unauthorized access (Privacy breaches targeting the confidentiality of the data) ➢ Data leakage (Cyberattacks such as Distributed Denial of Service (DDoS) attacks or malware infections.)
	Lack of standardization	➢ Outdated metadata ➢ Inconsistent metadata
Integration	Incorporating wrong data into the maps	➢ Data compatibility issues ➢ Conflicting data schemas ➢ Poor data mapping techniques ➢ Semantic heterogeneity ➢ Data Inconsistencies attack (conflicts are intentionally introduced into the data chain)
Usage	Display false or wrong information	➢ Data misinterpretation ➢ Improper utilization of context ➢ Biased decision-making ➢ Lack of transparency

Table 9: List of TN-ITS Data Chain Vulnerabilities and Potential Attacks

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

5.2. Top level Vulnerabilities mitigations and Potential attacks countermeasures

The suggested mitigation measurements for vulnerabilities and countermeasures to potential attacks listed above are mentioned below.

I. Data Collection

To address these vulnerabilities, ensure the reliability of collected data and continuously monitor equipment performance and availability, it is crucial to implement robust quality control measures, stringent data validation protocols (based on quality criteria such as data latency and timeliness), and continuous sensor calibration processes.

In the stage of data collection should also be considered possible mitigations/countermeasures to attacks alike data manipulation, such as:

a) Implement strong data authentication mechanisms to detect unauthorized modifications;
b) Apply encryption techniques to protect the integrity of the data during collection, processing and storage;
c) Employ digital signatures or cryptographic hashing to ensure data integrity and prevent tampering.

II. Data Transformation

To ensure data integrity, privacy, and fairness, it is crucial to identify missing information, incorrect data, or inconsistencies using rigorous data validation techniques/procedures, implement bias detection and mitigation algorithms and privacy-preserving data processing techniques.

Some obvious suggestions for possible mitigations are a Multi-Stage Validation Process: Implement a multi-stage validation process that involves cross-referencing data from multiple sources to detect and correct any inconsistencies or inaccuracies during the transformation stage; and Regular Audits and Reviews: Conduct regular audits and reviews of the data transformation process to identify potential vulnerabilities and areas for improvement. These audits can help identify and address any security gaps or weaknesses in the data chain.

In the context of the previous suggestions, it is crucial to demonstrate to potential data access enablers stakeholders that the process of improving data does not exclusively fall upon data providers. Instead, it is a collaborative effort involving all actors within the TN-ITS data chain.

III. Data Exchange

To enhance data security and interoperability, encryption methods, access control mechanisms, standardized data formats and comprehensive metadata management frameworks should be adopted. Developing these standardized protocols for data exchange will ensure confidentiality, integrity, and consistency.

Certain malicious cyberattacks and privacy breach activities can also lead to actions aimed at disrupting or compromising the TN-ITS data chain, as mentioned earlier. Therefore, here are some suggested countermeasures to adopt:

a) Deploy robust firewall systems and intrusion detection/prevention systems to detect and block malicious network traffic;
b) Regularly update software and systems with the latest security patches to mitigate known vulnerabilities;

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

c) Conduct periodic penetration testing and vulnerability assessments to identify and address potential weaknesses;
d) Implement strict access controls and authentication mechanisms to limit access to sensitive data;
e) Apply data anonymization techniques to protect personal information and ensure compliance with privacy regulations;
f) Educate personnel about privacy best practices and enforce privacy policies within the organization.

To further ensure that this data chain stage is not compromised, map providers can also provide feedback to road authorities regarding the quality and accuracy of the data they receive. In this case, manual verification of entities, events or conditions can be the most reliable option to adopt.

IV. Data Integration

To ensure reliable data integration, efforts should be directed toward establishing standardized data models, semantic interoperability frameworks, data reconciliation mechanisms, and comprehensive data quality assessment protocols. Establishing strict access controls, authentication mechanisms, and encryption techniques will protect data during transmission and storage.

Data inconsistency attacks are also a type of attack where inconsistencies or conflicts are intentionally introduced into the data chain, leading to potentially misleading or unreliable information. Some of the possible countermeasures proposed by the TN-ITS community include:

a) Establish data validation and verification processes to detect and resolve inconsistencies or conflicts in the data;
b) Implement robust data governance practices to maintain data quality and integrity throughout the data chain;
c) Employ data reconciliation techniques to identify and resolve discrepancies between different data sources.

TN-ITS community suggests conducting regular audits, vulnerability assessments, and testing to identify and address potential weaknesses. Foster collaboration between stakeholders to promote data sharing and establish common standards for data integration. To identify data integration issues, the map providers can identify any issues or conflicts that may arise during the integration process.

V. Data Usage

To mitigate these risks, it is essential to implement explainable AI models, data validation methods specific to application domains, decision support systems (based on monitoring of service use statistics), and transparent governance frameworks for data usage. End-users can/should provide feedback on the accuracy and reliability of the digital maps they use and surveys of perceived quality by users (for more specific information see the following subchapter “Feedback Loop”). For that, should be provided training and education on data interpretation, context utilization, and ethical considerations to enhance data usage practices.

By implementing these measures, the trustworthiness, reliability, and overall quality of the TN-ITS data chain can be significantly improved, contributing to more effective and efficient applications in the field of transportation and infrastructure management.

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

In all stages of the TN-ITS data chain, a category of potential attacks must be taken into consideration, Malicious Entities. This more wide-ranging category encompasses all the previous potential attacks. However, here are a few more countermeasures to be considered throughout the lifecycle of the TN-ITS data chain.

a) Implement strong user authentication and authorization mechanisms to prevent unauthorized access;
b) Conduct background checks and vetting processes for individuals and organizations involved in the data chain;
c) Monitor and analyse user behaviour and network activities for any suspicious or anomalous behaviour.

These mitigations and countermeasures should be personalised to the specific needs and requirements of the TN-ITS data chain adopted, or not, depending on the reality of each Member State / Stakeholder. Regular reviews, updates, and collaboration with cybersecurity experts can further enhance the effectiveness of these measures in protecting the integrity and trustworthiness of the data chain.

5.3. Impact of the vulnerabilities and countermeasures on the data quality aspects

This subchapter aims to establish a relationship between vulnerabilities/countermeasures and their impact on data quality aspects/concepts (trust, data quality, integrity, security, and sovereignty). The following table illustrates this relationship.

(Where 1 in a cell indicates that there is an impact of the vulnerability on the corresponding data quality aspect. For simplicity, the weighting is not considered).

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

			Trust	quality	integrity	security	soverignity		Impact (%)	
Collection	Incorrect data input	➢ Data tampering	1	1					2	50
		➢ Sensor inaccuracies	1	1					2	
		➢ Inadequate coverage	1	1					2	
		➢ Data provenance	1		1	1	1		4	
Processing	Incorrect standards or data values	➢ Algorithmic biases	1	1	1	1	1		5	95
		➢ Erroneous data transformations	1	1	1	1	1		5	
		➢ Inadequate data anonymization techniques	1		1	1	1		4	
		➢ Computational resource limitations	1	1	1	1	1		5	
Exchange	Malicious Data Injection	➢ Unauthorized access	1	1	1	1	1		5	1
		➢ Data leakage	1	1	1	1	1		5	
	Lack of standardization	➢ Outdated metadata	1		1		1		3	60
		➢ Inconsistent metadata	1		1		1		3	
Integration	Incorporating wrong data into the maps	➢ Data compatibility issues	1	1	1	1	1		5	100
		➢ Conflicting data schemas	1	1	1	1	1		5	
		➢ Poor data mapping techniques	1	1	1	1	1		5	
		➢ Semantic heterogeneity	1	1	1	1	1		5	
Usage	Display false or wrong information	➢ Data misinterpretation	1	1	1	1	1		5	95
		➢ Improper utilization of context	1	1	1	1	1		5	
		➢ Biased decision-making	1	1	1	1	1		5	
		➢ Lack of transparency	1		1	1	1		4	
		Importance	20	15	17	15	17			

Table 10: Impact of the TN-ITS Vulnerabilities and Countermeasures on the Data Quality Aspects/Concepts

Certainly, 'trust' is impacted by all vulnerabilities and countermeasures. As trust is the major differentiator for TN-ITS data compared to other data sources, it requires careful mitigation of all vulnerabilities. Data integrity is the second most crucial aspect that demands attention.

The greatest impact (relatively) of bad data quality is caused by the 'exchange' and 'integration' stages. This impact is calculated by adding the results vertically and dividing by the maximum number of points that can be obtained, expressed as a percentage: 100% means that all vulnerabilities impact the data quality in that specific data chain stage.

5.4. Stakeholders' major responsibility for Vulnerabilities / Countermeasures

The following table is a first assessment of the major stakeholder's responsibilities to control the vulnerabilities and/or countermeasures.

(Where 1 in a cell indicates that the respective stakeholder category (providers, access enablers, consumer, and end-user) will have a certain level of responsibility in the adoption of the corresponding vulnerability/countermeasure. For simplicity, the weighting is not considered).

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

			Stakeholder major responsibility			
			Data provider	Data access enabler	Data consumer	Road end users
Collection	Incorrect data input	➢ **Data tampering**	1			
		➢ Sensor inaccuracies	1			
		➢ Inadequate coverage	1			
		➢ Data provenance	1	1		
Processing	Incorrect standards or data values	➢ Algorithmic biases			1	
		➢ Erroneous data transformations			1	
		➢ Inadequate data anonymization techniques			1	
		➢ Computational resource limitations			1	
Exchange	Malicious Data Injection	➢ Unauthorized access		1		
		➢ Data leakage	1	1	1	1
	Lack of standardization	➢ Outdated metadata	1	1		
		➢ Inconsistent metadata	1	1		
Integration	Incorporating wrong data into the maps	➢ Data compatibility issues	1	1	1	
		➢ Conflicting data schemas	1	1	1	
		➢ Poor data mapping techniques			1	
		➢ Semantic heterogeneity	1		1	1
Usage	Display false or wrong information	➢ Data misinterpretation			1	1
		➢ Improper utilization of context			1	1
		➢ Biased decision-making				1
		➢ Lack of transparency	1	1	1	

Table 11: TN-ITS Stakeholders major responsibility on Vulnerabilities / Countermeasures

The above table will also be extremely important in the upcoming analysis/study to be implemented in the following Milestone (4.2.7) of this task. Understanding the responsibility of each stakeholder in the data chain to adopt vulnerability mitigation measures and implement countermeasures against potential attacks is crucial. This way, the TN-ITS community will know whom to approach for advice in adopting these measures to achieve a more reliable and trustworthy data chain.

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

6. Conclusions and next steps

6.1. Conclusion

This milestone deliverable M4.2.6 is a recapitulation of already published thoughts and concepts on how to approach data quality and aspects of enhancing the data chain. It represents the output or inventory of work conducted within a restricted timeframe. This task commenced later than initially planned, given that the task leader's position remained vacant until January 2023.

Relevant standards, regulations and projects that dealt with data and service quality were researched and summed up. A recapitulated of the findings made in the TN-ITS GO CEF project and presented a short history of the evolution of the data chain.

This document presented progress in defining a more generic data chain concept, bringing it from a ‘linear’ to a ‘circular’ representation, more in line with TM2.0 findings.

It clearly defines in more detail the aspects of the data chain -trust, data quality, integrity, security, and sovereignty. A more structured approach was presented on the vulnerabilities, their impacts, and top-level mitigations.

Finally, an exercise was executed to use the EU-EIP quality levelling approach. Although it is fully in line with earlier publications, this model is still very heuristic.

6.2. Next steps

The next steps will lead to the completion of deliverable M4.2.7.

It will consolidate all the insights and information gathered to develop a logical deduction, resulting in more detailed assessment methods for data quality aspects such as trust, quality, integrity, sovereignty, and security across the data chain. The objective is to identify potential areas for certifications (Trust and Quality) and explore the possibility of additional TN-ITS data and services to support the trust assessment method.

This forthcoming deliverable will also focus on defining requirements, identifying tools and best practices for deploying data evaluation tools for the TN-ITS standard trust assessment method. It will address the quality system and define levels of implementation for the necessary tools to ensure the data aspects of the TN-ITS data chain.

Some outlining methods for preserving the quality of the data will also be considered in M4.2.7, such as:

a) Continuous monitoring of equipment performance and availability;
b) Manual verification of entities, events or conditions;
c) Monitoring of data completeness and latency;
d) Monitoring of timeliness and data completeness;
e) Surveys of perceived quality by users;
f) Collection of direct user feedback;
g) Monitoring of service use statistics.

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

6.3. The Optimal TN-ITS Data Chain Quality System

The TN-ITS Data Chain Framework allows researchers, professionals, or academics to address the map related data assessment problem more comprehensively and in a structured manner, facilitating analysis and informed decision-making.
Moreover, the framework also helps identify gaps or areas that require more attention, enabling continuous improvements in the map related data assessment process.

In the upcoming Milestone (4.2.7) of Task 4.2.4, the identified gaps or areas that require further improvement will be subject to study and an optimal TN-ITS Data Chain Quality System will be suggested. This framework will suggest a possible combined approach from different components and different sources, such as:

- **Quality Criteria** (Level of Services and Data Quality Criteria) listed previously in this report from TN-ITS GO and EU-EIP;
- **Quality Levels / Requirements** from TN-ITS GO and EU-EIP;
- The six **Data Chain Concepts** (Trust, Quality, Integrity, Security, Sovereignty and Feedback Loop);
- Principles from **TM2.0 models** of cooperation;
- Weight of impact of the vulnerabilities and countermeasures on the data quality aspects;
- Among others.

This integrated approach will aim to provide a holistic view of how these elements work together to ensure the effectiveness and reliability of our milestone's data assessment methodology and to create a coherent and systematic evaluation system.

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