Digital Road Operator Information and Data Strategy (DROIDS)

Handling of trust and security in digital road infrastructure

Deliverable D4.1 Version 1.2

Date 05/11/2025

Digital Road Operator Information and Data Strategy (DROIDS)

D4.1 Handling of trust and security in digital road infrastructure

Due date of deliverable: 30/04/2025

Actual submission date: 05/11/2025

Start date of project:
15th of September 2023

End date of project:
14th of September 2025

Author(s) of this deliverable:
Siddartha Khastgir, University of Warwick
Dodoiu Tudor, University of Warwick

Version: 1.2

Executive summary

Trust and security in digital road infrastructure are important topics in ensuring a successful digitalisation process. This report provides a trust model adapted from the field of safety of Automated Driving Systems.

The proposed paradigm is that of “trust in” the system, which entails that the system behaves as expected, and “trust with” the system, which focuses on ensuring the proper use of the system within its limitations. Some of the key aspects identified around digitalisation are knowledge, certification, technical awareness, capacity and willingness.

This model was presented to members of NRAs as well as experts in a workshop. The results of the workshop were applied along with the trust model to create recommended actions and policies which can be implemented to solve certain issues that can appear with the “trust in” or “trust with” categories

Key recommendations include ensuring standard enforcement, as well as active participation in standardisation activities, as well as training and capacity building.

Glossary

ADS	Automated Driving System
ADAS	Advanced Driver-assistance System
AI	Artificial Intelligence
AIM	Asset Information Modelling
ALKS	Automated Lane Keeping System
BIM	Building Information Modelling
CAV	Connected and Autonomous Vehicles
CCAM	Cooperative, Connected, and Automated Mobility
CEDR	Conference of European Directors of Roads
DROIDS	Digital Road Operator Information and Data Strategy project funded by CEDR
DT	Digital Twin
EC	European Commission
EU	European Union
GPS	Global Positioning System
HD	High Definition
ISO	International Organization for Standardisation
IoT	Internet of Things
n.d.	No date mentioned in the reference
NRA	National Road Authority. NRA is often used in Europe. This study uses a term “road operator” that also includes NRAs.
ODD	Operational Design Domain
UN	United Nations
VRU	Vulnerable Road Users

Table of contents

Contents

List of Tables

List of Figures

1 Introduction

This report is focused on presenting a trust model that NRAs can use to better understand trust interactions in the space of digitalisation. Trust is a vital topic in the space of data and digitalisation. Large amounts of data of varying types are needed in current applications and potentially more would be needed in future application. Trust is vital across the lifecycle of this data. Starting from data collection, users need to be able to trust that their data is used appropriately to provide it. Processing the data after it is collected needs to be done in a trusted manner to ensure that the appropriate conclusions can be drawn from it. Finally, the end-users need to trust in the result of the system using the data. Applications explored in other WP where trust is particularly important are AIM and BIM.

The trust model proposing addressing the trust issue from a “trust with” and a “trust in” data perspective to create a comprehensive plan of addressing trust. This formed the basis of the analysis, alongside reviewing literature and standards and input from the workshop held as part of the WP.

- Chapter 2 presents the purpose and scope of the document.
- Chapter 3 presents the trust model and how it applies to the context of digitalisation, with a focus on trust with and trust in systems and data.
- Chapter 4 provides the results and key takeaways of the workshop on trust conducted, as well as how they influenced the recommendations given.
- Chapter 5 consists of a list of recommendations that arise from the trust model and the workshop from the previous chapters. These recommendations are sorted into two categories, based on the aspect of the trust model they are most relevant to.
- Chapter 6 provides a conclusion to the document as well as details on how the recommendations should be prioritised.

2 Purpose and Scope

The aim of the DROIDS project is to provide road operators with increased knowledge and support with relation to digitalisation, with a focus on the European context. The process of managing both physical and digital road infrastructure is a new challenge which needs to be navigated with care, with trust being one of the important factors to consider.

This deliverable presents the research results carried out during Task 4.1: "Establishing factors and framework enabling trust information" and Task 4.2: "Definition of information content classification and distribution scheme for use cases". Task 4.1 was focused on establishing factors influencing "trust in the information" and "trust with the information", and task 4.2 was focused on applying the trust framework identified in the previous task to create an information distribution framework.

This deliverable aims to answer the following questions shown in Table 1 below.

Table 1: DROIDS project Work Package 4 Trusted service provisioning research questions

RQ		Chapter
RQ15	How can the distribution of this information be made resilient and trustworthy enough to ensure that vehicles and drivers have the information required to ensure that roads can be used safely?	3
RQ17	What kind of information will be particularly critical to have verified, and how should trust in the authoritative information be ensured?	3
RQ18	What information falls into the different security categories?	5
RQ19	How can NRAs ensure that data is efficiently distributed to those who need to see it, and how can NRAs ensure that consumers of the information are able to trust its authenticity / veracity?	5

In addition to answering these research questions, the report will also cover the results of Workshop 4.1, which was aimed at understanding an NRA's perspective on trust and on the trust model presented.

Key terminology

1. It is to be noted that **the term "road operator"** is used in this deliverable to describe any public or private entity that is responsible for the planning, maintenance and management of the road, including management of traffic flows. The term "road operator" therefore also covers road authorities that are public authorities responsible for similar tasks. The term has been here adapted from the European Commission delegated regulation (EU) 2022/670 of real-time traffic information services (EC 2022). The term NRA is often used in Europe to describe a Member State national authority that is responsible for the previously mentioned tasks; in this study, the term road operator is also used to cover NRAs.

2. While the concept of Digital Twin has numerous definitions, the **DROIDS definition of Digital Twin** was formulated which is as follows:

   "**Road transport Digital Twin** is a realistic virtual representation of the real-world physical road transport systems. The road transport Digital Twin can include, depending of a purpose and defined functional scope, digital representation of elements such as road infrastructure, traffic with vehicles and pedestrians, road environment, traffic regulations and restrictions as well as land use. The road transport Digital Twin has a bidirectional real-time data connection between the physical and the digital representation. It can support road operator decision making with dynamic monitoring, analysis, and predictive modelling capabilities of the road transport systems that enable road operators for instance to enhance traffic flow, road safety, infrastructure asset management and sustainability or to facilitate automated driving or other future purposes. "

   The DROIDS definition of Digital Twin will be iteratively reviewed throughout the project based on input and feedback from the project stakeholders. Therefore, the above-mentioned DT definition can be changed in later (DROIDS) deliverable reports. The final definition will be published in the final report (Data Strategy).

3 Trust model

Before discussing the details of the trust model, it is important to define what trust is. We use an adapted definition of trust (Lee and See 2004) as “a history dependent attitude that an agent will help achieve an individual’s goals in a situation characterised by uncertainty and vulnerability”. The historical aspect was added to the definition to reflect how knowledge of a system’s capabilities and limitations affects an individual’s attitude towards the system. Various factors influence trust, however for the digitalisation, significant elements include knowledge, certification, technical awareness, capacity and willingness.

For an organisation to be able to reap the true benefits of digitalisation, it needs to develop an appropriate level of trust to ensure correct use. We propose that instead of treating trust as a monolithic construct to instead consider two forms of trust:

- Trust ***in*** the system
- Trust ***with*** the system

By system in this context, we refer to informational systems, as well as their components. “Trust in the system” means an organisation’s trust in the capabilities of the system or in the system’s ability to do what it is supposed to do. When applied to data this refers to trust that the data is accurate and correct for its intended purpose. “Trust with the system” means the user’s awareness or attitude towards the limitations of the system and their ability to adapt their usage of the system to accommodate the limitations of the system to deliver the expected benefit. This extends to ensuring that members of the organisation are aware of these limitations and are able to adapt to them. In the context of data, trust with it is the user’s awareness of its limitations and degree of correctness, as well as the ability to ensure that the data can be used for its intended purpose. This paradigm of trust was adapted from a paradigm of trust for the trust in the safety of autonomous driving systems (Khastgir 2019), as shown in Figure 1. To ensure that vehicles and drivers have the information required to ensure that roads can be used safely in this context can is equivalent to ensuring that these users can trust *in* the system and that they can be trusted *with* the system.

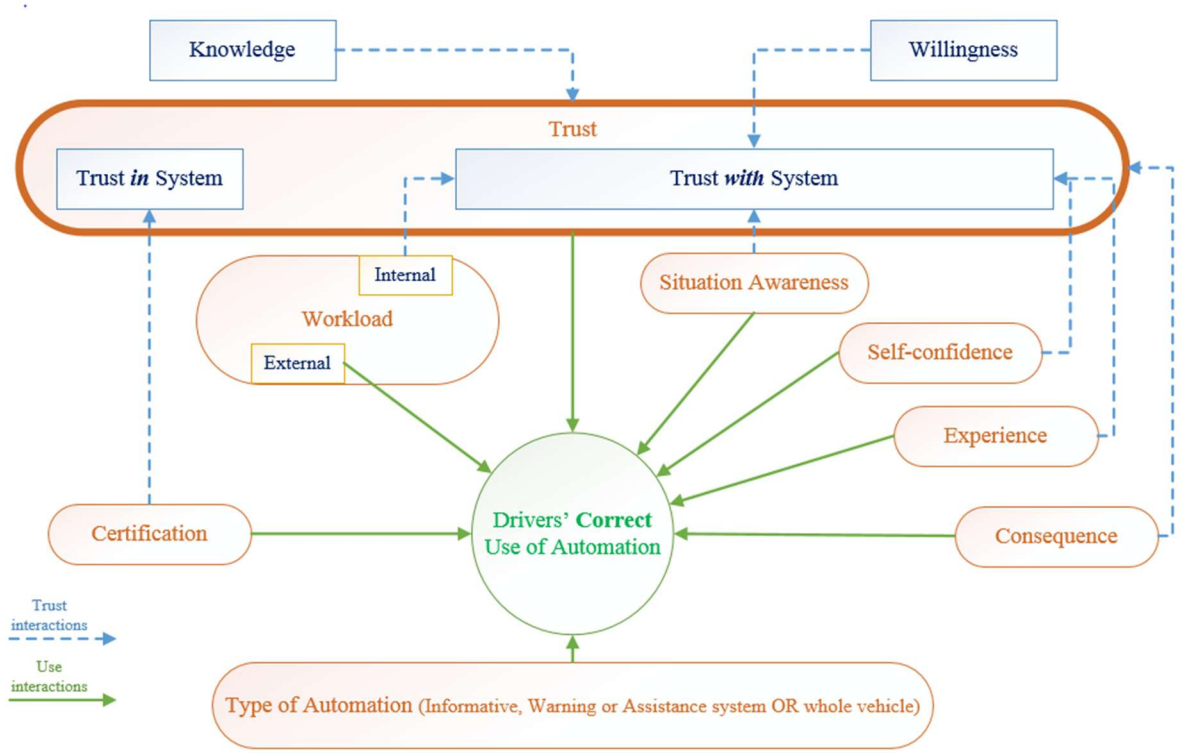

Figure 1 Framework for driver-automarion interaction in automated systems in vehicles

Knowledge about the capabilities and the current state of the system encourage the development of the system. If the knowledge is factually correct it leads to the development of "appropriate trust", leading to the correct use of the system or data while avoiding introducing a false perception or capability. The accuracy of this knowledge leads to the formation of a mental model for the users of the system. A correct mental model of the system forms the basis for appropriate trust in/with the system for a particular user. At an organisational level this is mirrored through the organisation's policies and procedures to ensure that members follow a similar mental model.

The knowledge can be categoriesed into three the following proposed categories:

- Static knowledge: Understanding of the working of the system
- Real time knowledge: Real time information about the system
- Internal mental model: Understanding or influence of external sources that system behaves as expected.

Information about the true capabilities of a system leads to the development of "appropriate tust", which helps form rule-based and knowledge-based decisions. Another dimension to knowledge is the accuracy of information. Lack of knowledge of how particular data was processed can lead to misuse of the data, and reduced trust with the system.

Knowledge is one of the key aspects that NRAs need to tackle roads can be used safely. This knowledge is built from different information, and as such, drivers and other road users will require different types of information than Autonomous Driving Systems. For road users, the importance of providing information lies in helping them build trust *with* the road, to ensure that their internal mental model matches the real-world conditions to ensure that they can adapt appropriately. On the other hand, information that an ADAS or ADS requires is much more focused on building trust *in* the system. Here, the most important aspect of the information is

the accuracy of the information to ensure the right Static or Real time knowledge required of the system. HD maps, discussed further in DROIDS Deliverable 3.4.(Shubham Soni et al. 2025), is one of the types of information that needs to be accurate to ensure appropriate knowledge.

Certification is another important concept. IEEE 24765 defines “certification” as “a written guarantee that a system or component complies with its specified requirements and is acceptable for operational use”. Certification establishes a clear boundry between safe and unsafe systems. Unlike the automotive field, there is less legislation on how data collection, processing and use can be certified. ISO 9001 is one standard for quality management systems that is widley implemented across Europe. TIARA report : National Road Authority guidance on legal and ethical use of data provides a more indepth analysis of data quality. Results can be achieved by defining characteristics of the data lifecycle whith a third party to verify the certification through thorough testing. Both the data itself and the proccesses related to it can undergo certification to ensure trust in/with the system. Certification is therefore a powerful tool NRAs can use, wether the NRA acts as the certification body, or through requiring third party certification in data provided to them, to the public or to ADS through OEMs.

Technical awareness within an organisation is a key factor in creating trust with the systems, as the technical expertiese can guide policy to ensure best practice is maintained. This is especially relevant in fast moving fields where certain aspects of best practice can evolve faster than standards or legislation, such as cybersecurity. This also applies to the technical understanding of current methods for data collection, processing and use, ensuring that the best fit method is chosen for the intended application, improving the trust in the system. This techical awareness is highly dependent on the human resources of an organisation, and as such the importance of spreading the repelvant aspects of it through policies into the organisation needs to be highlighted.

Anothter two important characteristics are capacity and wilingness. By capacity we refer to the ability of an NRA to take actions to improve either the trust in a system or trust with the system. Willingness is the motivation to take these actions. Both are required to ensure that trust in the system and trust with the system is maintained. At the same time, both of them are limited resources that need to be allocated based on the NRA’s priorities.

4 Workshop

The workshop on “Trust across the service provisioning model” was conducted on the 24th of January 2025. The aim of the workshop was to two-fold, to understand the perception of NRAs of what factors are important when it comes to “trust in” and “trust with” data, as well as their view of the trust framework and how it is applied.

The workshop participants were CEDR members, i.e. road operators, as well as other members from the CEDR Call 2022 Data projects of DROIDS on digital road infrastructure, PRESORT on third-party data and TIARA on trustworthy and secure data infrastructure. The workshop consisted of three parts.

The first part consisted of a 20-minute presentation of the trust framework used, as shown in chapter 3. This was focused on priming the participants in the “trust in” versus “trust with”. The characteristics of both were highlighted to the participants, as well as how they apply in the context of informational systems. This also included an overview of the different kinds of knowledge and how they link back into the trust model.

The second part of the workshop was a 30-minute group discussion session. The participants were split into three groups, with each group having at least one CEDR member. The groups were asked to answer two questions:

- How can information be collected in a trusted manner?
- How do we trust the entities collecting this information?

These questions were aimed at the data collection aspect as it is removed from the agencies using the data by one or more degrees of separation. The questions also aimed to prompt the participants to think both about the different entities that handle the data, but also about the data itself.

The third part of the workshop consisted in a 10-minute reflection, where the three groups providing conclusions on their discussions to the rest of the groups. The unique points that were brought up in the discussion are presented below:

- It is important to recognise that OEMs, Service providers and NRAs have different and sometimes conflicting interests. These conflicts can cause breaches of trust between the organisations.
- Contracts and service level agreements can ensure trust between entities; however, loopholes or mistakes could lead to unintended results such as data that is not useful to the NRA.
- When a relationship is already established, system auditing and data authentication are processes that can ensure the data authenticity.
- Regulations are important, as organisations are less likely to breach them.
- There are inherent risks with service provisioning, and NRAs need to acknowledge these risks and take appropriate actions to balance the risks taken.
- The reputation of a service provider was mentioned as an important factor in trusting entities collecting the information.
- European data spaces were mentioned as a good example on how data exchanges can happen in a trusted manner

The results of the discussion were fed back into the trust model to capture the concerns of the NRAs. The discussion was also useful in identifying the different type of data. NRAs need to be able to trust data from Service providers, even when the data collection was handled through other organisations. As such, the trust an NRA puts in the data needs to be calibrated based on the pool of knowledge that the organisation has. This should include local and European Union laws and regulations, type of contract between the entities, past experiences with the provider or similar providers and the familiarity with the technologies used. All of these should be used by the NRA to calibrate their trust in the data by recognizing the risks involved and managing them. After identifying these risks, the NRAs should consider mitigating actions to ensure that the data they will have access to can be trusted, whether the data is acquired straight from OEMs, service providers that have collated data from multiple sources, or other NRAs. This can ensure that the organisation can be “trusted with” the data through recognising the risks and potential issues that can arise but also have “trust in” the data from the organisations providing it.

A highlight from the discussion was on the type of data that NRAs were concerned about, with the important factors mentioned being the organisations providing the data, rather than specific contents of the data. The participants had been primed from a previous workshop in the same day, focused on data acquisition and the different contracts used to quire the data. Some of the discussion from the previous workshop spilled into the discussion from this workshop. This needs to be kept in mind as the results of the results are slightly skewed due to this, although the focus on the relationship between the NRAs and Service Providers kick-started the different group discussions.

5 Recommendations

The recommendations section is split into two sections, one for recommendations that mainly help with the “trust in” issues (recommendations starting in 4.1.) and recommendations that deal with the “trust with” issues (recommendations starting in 4.2.). It should be noted that some recommendations fall somewhere in between the two, so they have been placed in the category in which they would have the most effect. Additionally, one element that was taken into consideration was the maturity of the issue at the moment of writing for the general case. In cases where changes to the underlying issues would lead to a change in the recommendation will be highlighted where relevant.

5.1 “Trust in” Recommendations

These recommendations aim to improve the “trust in” aspect of the system. This is tackled through both knowledge of the system as a whole and its components, as well as certification of different aspects of the system. The aim of the recommendations is to ensure that the system matches the expected behaviour and can deliver benefits as expected. This category of recommendations focuses on, but is not formed entirely of, actions that need to be taken during the procurement process, or while forming agreements with third parties. A lot of recommendations in this category are directly or indirectly related to cybersecurity topics. When implementing these recommendations, it is expected that an expert in the field or at least a person with knowledge in the field should be consulted to determine the relevance and specific of implementing that recommendation. Depending on the maturity of training and capacity building (see R.2.15.) this may be a member of the NRA, or a third party.

R 4.1.1. Reputation-based trust

There are many factors that play a role in the trust in the data that an organisation should have. One of the most important aspects of this is the source of the data, in this case the Service Provider. This link is important as the interactions and agreements made between the Service Provider and the NRAs need to be regulated based on the trust in the Service Provider. One way to calibrate this trust relationship is through the reputation of the Service Provider (Ramya et al. 2021).This reputation can be internal, based on previous interactions with them. Based on these, lessons learned should be applied to future interactions in the case that they have not been egregious breaches of trust. Negative previous experiences may lead to needing to introduce additional measures to ensure those experiences do not repeat, such as R 4.1.4. independent Certification. Similarly, external reputation could lead to the same conclusions, however, the reliability of it is not as strong as past experiences.

R 4.1.2. Identify potential conflicts of interest with OEMs

Depending on the scope of the NRA, part of the organisation may act as a regulatory body within the automotive space. Due to this there is an inherent potential for conflicts of interest between OEMs and NRAs, especially when the OEM falls within its regulatory purview. The areas where conflicts of interest should be identified, even in cases where it’s not the regulatory part of the body is engaging with the OEM. Where there are risks identified, mitigating actions should be taken to ensure that the potential consequences are minimised. One case of interest where this may happen is an OEM attempting to exaggerate their system’s performance, as there are historical incidences of this, such as the Volkswagen emissions scandal (Jung and Sharon 2019). The mitigating actions that can be taken can address both trust in and trust with issues, with R 4.1.4 or R 4.2.7 being

particularly important in the given example.

R 4.1.4. Independent or Third-Party Certification

Some projects that involve conflicts of interest, where there are reputational concerns or where the quality of the data is particularly important, the NRA could request that the service providers undergo a third-party certification process before beginning service to ensure the quality of the data or that aspects of data collection or processing follow an expected pattern that is critical to the project. This protects the NRA, as well as providing trust in the process. While a third-party may not be necessary, there are many benefits as this allows for an objective evaluation, reducing the amount of bias in the process. Additionally in cases where the Service Provider would like to contest the results of the certification, the independent aspect would ensure the validity of the original results.

Another argument for Third-party Certification would be in cases where the data would be used in shared data spaces such as European Data Spaces. Here, the focus would be for the service provider to prove that they are compliant with the requirements brought by the data space. This enhances not only the trust in the data but also trust in the data space in general.

R 4.1.6. Ensure adherence to standards and participation in standardisation activities.

Standards are an important part of ensuring cooperation with other organisations and compliance with best practice. Multiple organisations pass these standards at different levels, European, national or international. Some institutions can also localise broad international standards into national ones. As such, it is important to identify which standards are relevant and ensure adherence to them. In the case of competing standards, a decision may need to be made as which one is more relevant, based on the issuing organisation, date of publication, wider acceptance and relevance.

The opposite issue where no standards are available in the space may also arise. In this case, or in cases where relevant standards are not effective, NRAs could consider joining standardisation activities in the area, especially if they have expertise in the area. There are many benefits to participation in these activities, from ensuring that the standard remains relevant for the use cases most relevant to the NRA, to helping with early adoption of the standard and helping with its adoption.

It is not enough for only the NRA to comply with relevant standards, but NRAs should encourage or require third parties to be compliant with the same standards. The benefits of this are both technical and financial, as the interoperability brought by the standards leads to less technical work needed. From a trust perspective, it ensures not only that the NRA is using best practices, but also that the third parties that collect and/or process data also follow them. This improves the credibility of the data, as well as helping improve trust with the data.

R 4.1.7. Use of Standardised Data Formats

In the case where there are no relevant standards, or sometimes competing standards, steps can be taken to ensure that data is stored and used in the same standardised format across different projects. This brings a few technical benefits as it enables interoperability between datasets and consistency. From a trust perspective, ensuring that data follows a predetermined format enhances the trust in the data through decreasing the likelihood of miscommunication leading to wrong assumptions being made about the data.

The data formats should be consistent across the organisation where possible, and as such, decisions need to be made at the organisation level as the form that certain data types should be stored and processed. Data sources should be audited to ensure adherence to these formats, and appropriate changes made in the case that they don't match the standardised format.

R 4.1.8. System Auditing

To ensure adherence to standards and best practices, System Audits can be performed. The audits involve assessing an organisation's information systems to ensure legal compliance and adherence to standards and best practice. This furthers recommendations R 4.1.6 and R 4.1.7., to ensure that the standardisation goes past policy and is implemented to its fullest extent within different projects. This recommendation becomes more relevant the larger the organisation as there is more opportunity for issues in communication and compliance to arise.

R 4.1.9. Data Authentication

Data Authentication, also known as Message Authentication, is the process of confirming the origin and integrity of data. Implementing this process as a requirement for third-party can ensure that the data has not been tampered with, and that only authorised parties have provided it.

The importance of this process will depend on the type of data that is being acquired and its sources. The situations where this becomes important in ensuring trust in the data is situations where data is being acquired on a continuous or regular basis or where there are many sources for the data. In case of continuous or regular data transfer, data authentication ensures trust in the completeness and accuracy of the data. The process ensures that if data is lost in transit there is a clear trail, which can help in recovering the missing segments if necessary. The other principal benefit is in preventing on-path attacks (Wells et al. 2006) from malicious actors. In the other case, where multiple parties are involved, data authentication is important to ensure traceability to the relevant party. Additionally, message authentication can prevent spoofing attempts, where an attacker impersonates a trusted source. Even in cases where spoofing occurs due to social engineering, the data introduced by the attacker can be identified later and removed if necessary.

From a technical standpoint there are multiple methods to achieve data authentication, with the most common being through a Message Authentication Code (MAC), also known as Message Integrity Code (MIC). This cryptographic technique involves including a MIC along with the message, which the receiver can compare with a MIC they generated to ensure the message is authentic and in its integrity. There are many algorithms that can be used to implement this process, highlighted in standards such as ISO/IEC 9797-1, ISO/IEC 9797-2, ISO/IEC 9797-3 or ISO/IEC 29192-6.

The recommendation therefore in this area is that in cases where data is acquired on a continuous or regular basis, or from multiple sources, a data authentication process be implemented. When determining the requirements for data acquisition, technical staff or a cybersecurity expert should be consulted to determine if data authentication is required, and if so, what algorithm should be used and agreed on with the relevant parties.

R 4.1.10. Maintain Access Control and Audit Trails

When storing data for any amount of time, to ensure that it has not been modified Access

Control protocols should be implemented. The aim is to ensure that only authorized personnel and parties have access to the appropriate data, along with the necessary permissions to access, view, modify or delete data. While this is required to some extent to be GDPR compliant, depending on the type of data, this should extend past it. Another further step is to maintain logs for who is accessing what data and the operations being performed, to create an audit trail. The benefits of this are that in the case of unauthorised access to data, the affected and unaffected data can be distinguished. This is important both to ensure trust in the data, but also to ensure trust with the data.

Access Control is a widely spread policy already implemented by digital systems, however specialised uses may require a more in-depth analysis of the needs of the system, as well as the policies that govern Access Control, especially if data should be made available to third parties. The benefits of implementing a more sophisticated Access Control system that includes Audit Trails can extend beyond the scope of a single project or system, as such a one-time investment may lead to benefits across the organisation in multiple projects.

The recommendation is therefore that Access Control should be considered beyond the legal requirements. From a governance perspective, the policy on who, how and in what ways the data can be accessed should be clearly defined. Most organisations already have a high maturity of this, so a periodic assessment of the policy would be adequate. From a technical perspective, maintaining an Audit Trail for access should be considered as it can potentially limit and help assess the extent of damage caused by a hostile actor who has gained unauthorised access, most likely through social engineering if proper cybersecurity measures have been implemented.

R 4.1.14. Data Redundancy and Cross-Verification

Sometimes multiple sources are available to provide the same information. In these cases, Data Redundancy can be implemented by keeping the same data from multiple sources. This brings two major benefits. Firstly, in the cases where there are issues in the data, either due to issues with data collection or processing, or due to malicious attacks, there is another dataset that may not have been affected by those issues which can be used to replace the faulty data. Cross-Verification in this context can be used to identify faulty data and replace it to ensure trust in the data. Secondly, the redundant data, in combination with other recommendations such as data quality assessments (R 4.2.11.), can be used to determine the quality of a particular provider, which feeds back into reputation based-trust (R.1.14.).

The downside of keeping redundant data is that it may lead to increased costs due to increases in required storage spaces. To prevent this, redundant data could only be kept for a particular timeframe or at a reduced frequency, with the best solution being dependent on the type of data being used.

The recommendation is that where available, a portion of redundant data should be kept and used for Cross-Verification, especially where there could be issues with the principal data could arise. The amount and type of redundant being kept will depend on the application, as well as the source of the data.

5.2 *"Trust with" Recommendations*

These recommendations focus on improving the "trust with" aspect of the system. The aim of these recommendations is that the user is aware of the system's limitations and how to navigate them. The actions recommended in this category are formed of both actions that should be taken pre-emptively as well as actions that should be taken reactively based on circumstances.

R 4.2.1. Transparency of Data Collection and Processing

Transparency in data collection and processing is key in building public trust, as well as trust with the data provided (Wiencierz and Lünich 2022). When communicating to the public about safety it is vital to be able to prove the validity of the results. To be able to provide this justification, transparency in data collection and processing is a key aspect in helping the public understand the data that lead to results. If data is acquired through third parties, it may be important to require their processes to be transparent to an extent to be able to build a safety argument.

Another benefit in requiring transparency of third parties is that by understanding the data collection process can validate the data, as well as ensure that the organisation can be trusted with the data.

R 4.2.2. Develop clear requirements for data provisioning

The scope of data collection and processing may be too large or too expensive for an NRA to accomplish on its own. In these cases, data will need to be acquired from a Service provider, who may oversee data collection, processing and/or aggregation. In any case, the relationship with the Service Provider will be determined through the procurement process. It is important that during this process the NRA put clear requirements on the data but also the relationship to the Service Provider. This process will depend on the local legislation; however, these requirements should apply. R 4.1.4, R 4.1.6, R 4.1.8, R4.1.9, R1.1.14, R 4.2.1 and R 4.2.11. would all fall under some of the requirements that can be applied here.

While requirements will depend on the use case, a good amount of requirements would remain consistent across projects. These requirements will evolve through time, with past experiences providing lessons learned that can be applied to form new requirements. R 4.2.15 and R 4.2.14 are important in this case. These requirements should be part of capacity building, both from a technical and legal perspective, as well as be a focus to discuss with other NRAs, especially when there are common OEMs, Service Providers or stakeholders.

R 4.2.4. Assess risks associated with data

Risks associated with data will depend on the security categories the data will fall under. According to the GDPR, information can fall in one of the following three categories:

- Public data
- Personal data
- Sensitive personal data

The more sensitive the data, the more requirements are put on processing and its collection, therefore higher risks are associated with it. Many applications are unlikely to need personal data, such as HD maps.

One additional layer for data that should be considered is the timing of data collection, processing and use. There are three further categories of data based on this:

- Continuous Data – data which is received at short regular intervals
- Periodic Data – data which is received at long regular intervals
- One-off Data – data that is received once

Each type of data brings different types of risks. The trade-off is that security risks may appear with data received continuously, whereas one-off data acquisitions are at a higher risk for inaccuracies and may be more difficult to validate. These risks need to be balanced depending on the application that the data is needed for.

There are risks associated with data procurement and use that can affect projects in different ways if they come into fruition. These risks should be accounted for and mitigating actions should be taken to ensure that the chance of a risk occurring is minimised and the potential harm of the issue reduced. The next paragraphs deal with the most likely risks that should be considered.

Malware is a constant risk, and many cybersecurity measures can be taken to prevent it. One area of particular interest here is that malicious actors may be able to gain access to third-party trusted systems and introduce malware through that system. A recent occurrence of this was the Marks and Specer's cyberattack where ransomware was introduced by a trusted third party which was compromised through social engineering. As such, it is important to review the level of access that is given to Service Providers and the risks associated with those.

Data breaches are a risk that needs to be mitigated against. More mitigating actions should be taken to ensure that this does not occur when personal information is involved. Even when not storing the data, such as in situations where the service provider is the one responsible for it, data breaches on their end may still propagate issues back. Mitigating actions can be taken in both cases. For internal breaches, good cybersecurity practice and policies should help, however, for external breaches this may prove to be a more difficult challenge.

R 4.2.5. Document Assumptions and Use Constraints

When tools are being developed, assumptions on what the inputs and outputs of the tool should be, which leads to use constraints for the tool. These tools may be relevant past the project they are developed for, in which case they may be repurposed and used un other projects, where new data may be used as an input. To ensure that the tools remain usable in the future clear documentation is required.

The recommendation is that there should be a policy to create clear documentation which includes assumptions and use constraints to ensure future trust with these tools.

R 4.2.7. Validate Data Against Ground Truth

Validating data against verified information may be difficult, but in some cases it can provide important checks to ensure the data is correct. Implementing this would be best suited in situations where the data may be unreliable, either due to its source or method of collection, or in safety-critical applications.

There are two use-cases where this recommendation should be strongly considered.

Firstly, based on R 4.1.1., if the Service Provider is unreliable, this may be necessary to ensure that the data can be used without trust concerns. Secondly, any AI or mathematical based model application needs to be validated. If the level of data processing is transparent enough (R 4.2.1.), this may not be necessary if the Service Provider has proved a thorough process for validating their model.

R 4.2.8. Encourage Use of Complementary Data Sources

Complementary data sources can be used to derive information that would otherwise be unavailable from a single dataset. Another benefit is that they may contain parts that overlap, in which case they can be used for cross-validation. This is not applicable to all applications; however, it is relevant when acquiring raw data. Another benefit of using complementary data sources is that biased data or errors introduced by a particular source can be identified and accounted for. While less relevant when provisioning for more processed data, the use of complementary data sources can be included in the requirements for the service, as highlighted in R 4.2.2.

R 4.2.9. Define Baseline for Data Quality

Data Quality is a difficult thing to quantify, as different qualities of data need to be evaluated to determine whether it is suitable for its intended use. These qualities need to be measurable and quantifiable, with the minimum acceptable levels of these qualities forming the baseline. Not all properties are going to be applicable or relevant to all use cases, and as such, there is no one universal measure that can be used. Some qualities that could be considered (Fürber 2016) are accuracy, relevancy, timeliness, completeness, quantity, interoperability, accessibility, correctness.

After deciding on a baseline for data quality, this should be included as a requirement in data procurement process. This reduces the risks of procurement if the baselines have been set to ensure that the data is usable. Additionally, depending on the nature of the agreement, it may act as legal protection as if the Service Provider does not provide the data at the expected quality level there is a clear requirement that they would be breaching.

R 4.2.11. Periodic Data Quality Assessments

To ensure that data is fit for purpose in applications where live or regular data is received, assessing the quality of the data periodically would ensure that the data remains fit for purpose, and if not underlying issues can be identified. If a baseline for quality has not been set as per R 4.2.10., then a particular property of the data needs to be decided on to be able to assess the quality of the data.

Another reason to conduct periodic data quality assessments is that the relevance of data, as the needs for a dataset may change with time, therefore, not only should the data be assessed during the periodic quality assessments, but also if the required metrics are still relevant, and if so, if a new baseline quality should be set.

R 4.2.14. Cross-NRA cooperation

Encouraging Cross-NRA cooperation can lead to better results for all participants. While different NRAs or similar cover similar responsibilities across Europe, but not the same ones. Within the digital space there are a few areas that are relevant to most if not all however, and within these areas cooperation would be beneficial.

The first are of cooperation is related to the organisations that operate across Europe in the space. Because both OEMs and some Service Providers can fall into this category,

there can be valuable information about them that can be shared across NRAs such that known issues can be mitigated with prior knowledge from previous interactions. This is strongly linked to R 4.1.1.

The other area where cooperation can be helpful is around standardisation. Standardisation across Europe is important in improving interoperability between systems. The focus is on ensuring that standards are applied, as well as identifying areas where standardisation could occur, linked to R 4.1.6., as cooperation could speed up the process.

Finally, NRAs could also benefit from sharing key lessons learned from implementing new systems, such as a PKI system as suggested by the TIRAR project. There are many challenges when implementing new systems, so being aware of them and potential solutions could lead to lower costs and turnaround times.

R 4.2.15. Training and Capacity Building for NRAs

Most previous recommendations require staff with certain areas of technical expertise in fields such as cybersecurity, data management or project management. As suggested in the TIARA project, hiring skilled resources is a great way to accomplish this, but this may prove to be challenging, especially when the private sector may provide more benefits for similar expertise. One way to gain skilled resources is by offering training in relevant skills. Developing an expertise is also a valuable experience for the employee, acting as a great incentive to remain within the organisation (Elsafty and Oraby 2022). Retention is important when building capacity as employee turnover is expensive (Ladelsky and Lee 2023), without considering the lessons learned lost in the process. Another effective way to improve capacity is through effective knowledge sharing, which should be promoted through policies at an organisational level (Yeboah 2023).

6 Conclusions

Trust is a vast and nuanced topic. The trust model proposed in this report can help provide a better understanding of it, through the most important elements that form trust in and trust with a system or data. Each component forming trust contributes to the whole in different ways.

The workshop provides valuable insight into what issues NRAs are concerned with, along with potential solutions. The workshop participants were given background information on the trust model, with positive feedback given on its usefulness. The results of the workshop were used to validate the initial recommendations to ensure relevance and potential impact.

The recommendations given are a collection of actions or policies formed through an analysis of the trust model in coordination with the workshop. The list of recommendations has been given in no particular order as the priority and importance of each will not only depend on the implementing organisation, but also on the application. While individual consideration is important, there are two types of recommendations that should take priority over others. The first type is recommendations that deal with compliance with legal requirements and standards. These have the potential to cause the most detrimental or beneficial effects and therefore should be given a high priority. The other type of recommendations that should be given priority are those that deal with information security and cybersecurity, as they can heavily influence public trust.

References

Elsafty, Ashraf, and Mahmoud Oraby. 2022. 'The Impact of Training on Employee Retention'. *International Journal of Business and Management* 17 (5): 58. https://doi.org/10.5539/ijbm.v17n5p58.

Fürber, Christian. 2016. *Data Quality Management with Semantic Technologies*. 1st ed. 2016. SpringerLink Bücher. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-12225-6.

ISO. 2015. *9001:2015 'Quality Management Systems — Requirements'*.

ISO/IEC. 2011. *9797-3:2011 'Information Technology — Security Techniques — Message Authentication Codes (MACs) Part 3: Mechanisms Using a Universal Hash-Function'*.

ISO/IEC. 2019. *29192-6:2019 'Information Technology — Lightweight Cryptography Part 6: Message Authentication Codes (MACs)'*.

ISO/IEC. 2021. *9797-2:2021 'Information Security — Message Authentication Codes (MACs) Part 2: Mechanisms Using a Dedicated Hash-Function'*.

ISO/IEC/IEEE. 2017. *24765:2017 'Systems and Software Engineering — Vocabulary'*.

Jung, Jae C., and Elizabeth Sharon. 2019. 'The Volkswagen Emissions Scandal and Its Aftermath'. *Global Business and Organizational Excellence* 38 (4): 6–15. https://doi.org/10.1002/joe.21930.

Khastgir, Siddartha. 2019. 'Testing Automated Driving Systems to Calibrate Drivers' Trust'. In *Warwick Manufacturing Group*. PhD, University of Warwick. https://wrap.warwick.ac.uk/id/eprint/144215/.

Ladelsky, Limor Kessler, and Thomas William Lee. 2023. 'Effect of Risky Decision-Making and Job Satisfaction on Turnover Intention and Turnover Behavior among Information Technology Employees'. *International Journal of Organizational Analysis* 31 (7): 3553–81. https://doi.org/10.1108/IJOA-10-2022-3465.

Lee, J. D., and K. A. See. 2004. 'Trust in Automation: Designing for Appropriate Reliance'. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 46 (1): 50–80. https://doi.org/10.1518/hfes.46.1.50_30392.

Ramya, Govindaraj, Govindaraj Priya, Chowdhury Subrata, Dohyeun Kim, Duc Tan Tran, and Anh Ngoc Le. 2021. 'A Review on Various Applications of Reputation Based Trust Management'. *International Journal of Interactive Mobile Technologies (iJIM)* 15 (10): 87. https://doi.org/10.3991/ijim.v15i10.21645.

Shubham Soni, Sina Reshad, and Ilkka Kotilainen. 2025. *D3.4 Digital Twin Use Cases – Digital Transport Regulations, Opening New Roads, Automated Lane Level Navigation*.

Wells, Jason, Damien Hutchinson, and Justin Pierce. 2006. 'Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, Data Entry and Transaction Verification'. *Proceedings of the 6th Australian Information Security Management Conference* Edith Cowan University: 1st to 3rd December 2006. PDF. https://doi.org/10.4225/75/57B56646B8774.

Wiencierz, Christian, and Marco Lünich. 2022. 'Trust in Open Data Applications through Transparency'. *New Media & Society* 24 (8): 1751–70. https://doi.org/10.1177/1461444820979708.

Yeboah, Asiamah. 2023. 'Knowledge Sharing in Organization: A Systematic Review'. *Cogent Business & Management* 10 (1): 2195027. https://doi.org/10.1080/23311975.2023.2195027.