TELEMETRY [101119747]: Trustworthy mEthodologies, open knowLedgE & autoMated tools for sEcurity Testing of IoT software, haRdware & ecosYstems

D6.3 Data Management Plan (interim version)

Project Reference No	TELEMETRY - 101119747
Deliverable	D6.3
Work package	WP6: Project Management
Type	DMP – Data Management Plan
Dissemination Level	PU - Public (fully open)
Date	29/02/2024
Status	Final v1.0
Editor(s)	Joerg Abendroth (NOKIA)
Contributor(s)	Dmytro Prosvirin (ANT) Joerg Abendroth (NOKIA) Robert Seidl (NOKIA) De Lutijs Paolo (TIM) Steve Taylor (UoS)
Reviewer(s)	Martin Gilje Jaatun (SINTEF) Bernd Ludwig Wenning (MTU)
Document description	Approach to ensure compliance to legal and ethical constraints and FAIR principles for data management

Disclaimer

The TELEMETRY project is funded by the European Union under grant agreement ID 101119747. The information and views set out in this website are those of the TELEMETRY Consortium only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	07.01.2024	Initial draft	Joerg Abendroth
V0.5	18.02.2024	Use template, merge contributions	Joerg Abendroth
V0.87	20.02.2024	Version for review	Joerg Abendroth
V0.88	22.02.2024	Adding FAIR	Joerg Abendroth
V0.9	23.02.2024	Address review	Joerg Abendroth
V0.95	23.02.2024	Address review comments	Robert Seidl
V1.0	29.02.2024	Last Additions	Joerg Abendroth

Executive Summary

This document, the Data Management Plan of the TELEMETRY project, aims at defining the TELEMETRY data management policies and procedures. The scope includes both data that is handled during the course of project, as well as used in public documents, such as reports, deliverables or publications. Open Access is being favored and facilitated.

The use cases are set in a way that no customer data will be generated or collected, but some form of sensitive and personal data may exist. This data management plan outlines regulations and policies for data management, to be used in accordance with the governance structures documented in the Project Handbook[1] and Quality Assurance Plan.

Table of Contents

List of Figures

List of Tables

List of Terms and Abbreviations

Abbreviation	Definition
ATP aircraft	Advanced Turbo-Prop aircraft
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DUT	Device Under Test
EEA	European Economic Area
ERP	Enterprise Resource Planning
FAIR	Findable Accessible Interoperable Re-usable
FDR	Flight Data Recorder
FiaB	Factory-in-a-Box
HW	Hardware
IAM	Identity and Access-Control Management
IoT	Internet of Things
MES	Manufacturing Execution System
RAND	Reasonable and Non-Discriminatory Licensing
SBOM	Software Bill of Material
SW	Software
VPN	Virtual Private Network

Table 1: List of Terms and Abbreviations

1 Introduction

TELEMETRY will provide trustworthy tools that enable the continuous assessment of heterogenous, interlinked components & systems that constitute IoT ecosystems (interconnected IoT devices with hardware, software, services, and communications infrastructure). Addressing all aspects of their lifecycle, the TELEMETRY holistic methodology and toolkit incorporates testing for component development, testing & monitoring for component integration into systems, and testing & monitoring for operation of systems. TELEMETRY will deliver advances in cybersecurity testing and runtime monitoring through the use of novel machine learning models and algorithms for real-time anomaly detection; dynamic risk assessment to simulate likelihood and severity of threat consequences; reputation management and privacy-preserving data sharing across independent entities (e.g. supply chains); IoT device emulation and analysis environment and lightweight approaches for trusted updates; all of which promote a cycle of continuous improvement and assurance across design and runtime phases. TELEMETRY will leverage 3 exemplar use cases representing diverse, complex IoT ecosystems and IoT supply chains in aerospace, smart manufacturing, and telecommunications domains to drive the design and validation of the proposed tools and methodologies. This will lead to significant improvements with respect to accuracy of threat and vulnerability detection, response time and cost of testing and verification of IoT ecosystems. TELEMETRY will promote open source and knowledge sharing through engagement with relevant communities throughout the project for consultation, dissemination, and exploitation of its results.

1.1 Purpose and Scope

D6.2 is a report providing the data management plan (DMP) within the TELEMETRY project. During the course of the project new data sources might be used, and if so, the data management plan is to be updated. The final update will be by month 36.

1.2 Relation to other Work Packages and Deliverables

The DMP within WP1 touches all use cases and tool providers, because the Use Case Owners as data controllers need to set the correct data management policies and the tool providers as potential data processors need to adhere to the DMP.
Additionally, the Project Handbook[1] and Quality Assurance Plan defines roles and further procedures.

1.3 Methodology and Structure of the Deliverable

This deliverable pulls in the existing regulation the project is set in, namely the GDPR, and describes the project roles and processes how they relate. Specific analysis data use within the three use cases and their handling and requirements are addressed. Finally, the publication policy and adoption of FAIR principles within the project is explained.

2 Project Reports and Deliverables

This section outlines the handling of technical reports and project deliverables within the Data Management Plan (DMP). Partners collaborate on both project deliverables and technical reports, addressing the outcomes achieved by the project. To ensure the accuracy and correctness of these documents, all partners adhere to a well-defined Quality Assurance Plan[1], which follows the traditional four steps of the quality assurance process: Plan, Do, Check, and Act.

The Quality Assurance Plan outlines management procedures essential for ensuring the efficient production, maintenance, updating, distribution, and storage of project documents. It establishes objectives, roles and responsibilities, coordinates with other plans, and defines tasks and schedules. Concurrently, the DMP addresses specific issues concerning the appropriate use of data in deliverables, as well as in the research and administrative processes of the project. In summary, the Quality Assurance Plan governs the overall form and content of deliverables to ensure consistent usefulness and quality. In contrast, the DMP focuses exclusively on the handling of data, particularly personal and business data.

While there are no intentions to include personal data related to the use cases in the project's deliverables, it is the responsibility of the deliverable editor to confirm this stance with the project manager. If a situation arises where personal data may inadvertently be included, it will be addressed exceptionally, adhering to recommended practices for such circumstances.

3 Data Management

In this section, we describe the overall Information Management Governance structure for TELEMETRY.

The project will provide 3 use cases: Aerospace, Smart Manufacturing and Telecommunication. We aim not to use any personal data. Despite of that and in case a project partner will make use of personal data including sensitive data or data of special category, it is important to introduce an appropriate information governance structure as part of project compliance with GDPR Art. 30 (*Recording of processing activities*). In this section, we introduce basic structures which are to be put into place in such cases.

3.1 Data Types in TELEMETRY

The TELEMETRY consortium and its partners may possess various types of data. Generally, we don't differentiate between the origins and intentions behind this data. Nonetheless, safeguarding all personal data is crucial. Yet, it's beneficial to establish the following fundamental distinctions:

1. *Administrative Data*

    - Individual partners may retain personal information concerning their clients, as well as contact details for participants involved in TELEMETRY use cases. Certain details may hold commercial sensitivity for a particular partner. However, administrative data of this nature will not be exchanged among partners.

2. *Project Contact Data*

   - Furthermore, throughout the project's duration and directly relevant to its execution, project partners may gather data on individuals expressing interest in the project from a dissemination or exploitation standpoint. This Contact Data might be exchanged among partners, assuming the implementation of suitable data protection measures to safeguard any personal information involved.

3. *Research Data*

   - In use cases, data might be collected, exchanged between or across partners. This research data could be exchanged among partners, undergoing pseudonymization where the original partner retains the key. However, neither the key nor any individual's contact details will be disseminated to other partners.

4. *Secondary Data*

   - Personal data held by a partner, initially collected in a different setting, such as in a separate project, might prove valuable in a different project setting. For instance, attitudes toward privacy recorded in a different context could offer a useful baseline for investigation within TELEMETRY. These data, commonly termed secondary data, may only be shared with other partners if:

     i. Their proposed secondary use is consistent with their original purpose; or

     ii. Data subjects have provided additional consent; and

     iii. With a suitable Data Sharing (see below) agreement in place.

3.2 Information Governance Structure

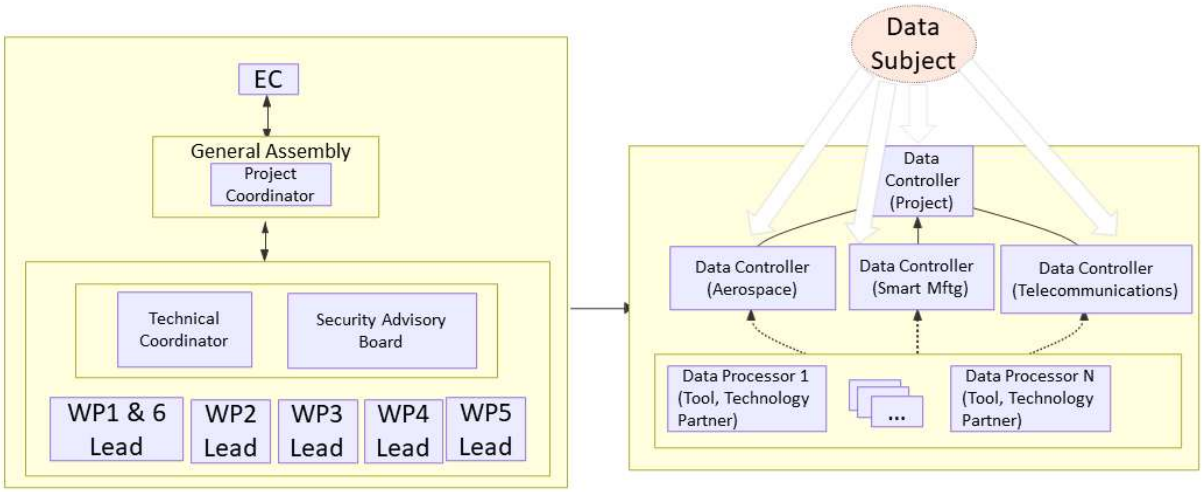

Figure 1: Overview of the Information Governance Structure in TELEMETRY

Figure 1 provides an overview of the Information Governance Structure within TELEMETRY and its alignment with the project management framework. The responsibility for Information Governance falls under the Project Management WP6 and directly reports to the General Assembly. Any requests from data subjects, including Subject Access Requests (SAR) or

concerns, should be directed either to the relevant Use Case Lead or directly to the Project Coordinator.

Both the Use Case Leads and the Project Coordinator serve as Data Controllers, each with distinct responsibilities as elaborated below.

3.3 Supervisory Authority

The GDPR (2016) Art. 51 defines the role of a Supervisory Authority; further, in the case of cross-border processing, a single Supervisory Authority may be appointed (Art. 56). This would generally be in the member state of the overall project data controller. For TELEMETRY Germany is being selected.

3.3.1 Default Jurisdiction

Following the provisions of GDPR (2016) Art. 56, the single Supervisory Authority for TELEMETRY will be Germany as the organizational headquarters of the Project Coordinator, Nokia Solutions and Networks GmbH & Co. KG (here Nokia), for the purposes of the TELEMETRY project. If required, and in cases where no other jurisdiction seems appropriate (see below), all data protection related matters will be managed in accordance with German law.

3.3.2 Data Subject Expectations

One exception to the default jurisdiction would be if there are specific deviations from German data protection law which may apply in the member state of an individual data subject. This may occur in the case of the use cases, for example. Any such differences will be considered as required and should be managed by the use case lead (the data controller for that use case) wherever possible.

3.3.2.1 Norway

Norway is not an EU member but is subject to the GDPR via the European Economic Area (EEA) agreement [2], and according to Commission decisions [3], personal data can flow to and from Norway without any safeguards being necessary.

3.3.2.2 The UK

With the United Kingdom's withdrawal from the EU complete, it has its own laws regarding data protection, but they are in line with the EU GDPR. At the time of writing (Feb 2024), the UK data protection legislation, the DPA (2018), is closely aligned with the GDPR. This law is in the process of being updated with the Data Protection Act 2023 just having had its second reading in the UK parliament (Dec 2023). The DPA 2023 is principally a refinement of the 2018 DPA and is intended to remain aligned with the EU GDPR. In consequence, it is not expected that any specific issues will arise. The status of UK data protection legislation will be reviewed and updated throughout the project as necessary.

3.3.2.3 Ukraine

The notes on https://www.dataguidance.com/notes/ukraine-data-protection-overview :

> *"Given Ukraine is not a part of the EU, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') does not directly apply in its territory. Meanwhile, according to the plan of actions related to fulfillment of the EU-Ukraine Association Agreement, as approved by the Cabinet of Ministers of Ukraine ('the Cabinet of Ministers') on October 25, 2017 No. 1106 (only available in Ukrainian here), Ukraine committed to bring its data protection legislation into compliance with the GDPR by May 25, 2018. In that respect, a draft Law on Personal Data Protection "…[4]…" ('the Draft Law') was developed and registered with the Parliament of Ukraine ('Parliament') in June*

> *2021. However, later on, the Draft Law was rejected by the Parliament on August 16, 2022. After the failure to adopt the Draft Law into law, another draft law "…[5].." ('the Second Draft Law') was registered with the Parliament on October 25, 2022. The Second Draft Law aims to bring the local data protection legislation into compliance with the GDPR, including the terminology, data subjects' rights, obligations of controllers and processors, etc. The Second Draft Law should pass all necessary steps to be adopted into law, i.e., it should undergo two hearings in the Parliament. To date, it is not clear when the whole law adoption process will be completed.*

are appropriate, with the clarification: But since Ukraine has undertaken to bring its legislation on the protection of personal data into compliance with the GDPR, therefore, during the course of the project, the Ukrainian partners of the project will be guided by the provisions of the GDPR in their project activities.

3.4 Data Controller

As defined in GDPR (2016) Art. 4(7) a

> *"'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*

As depicted in Figure 1, the Project Coordinator will assume the role of the overall Data Controller for the project, given their responsibility for directing the project's overarching direction. Consequently, any data subject inquiries should be directed to the Project Coordinator as the Data Controller. Required for success, robust communication channels between the coordinator and other consortium partners are needed.

For the individual use cases, each designated use case lead will function as a Data Controller for the specific activities within their use case. This designation arises from their authority in determining the (personal) data to be collected and the processing methods involved. Since use case partners are expected to align with the Project Coordinator regarding the overall scope and objectives of their use case, the Project Coordinator and the use case lead jointly serve as controllers (GDPR, 2016, Art. 26). Facilitating effective information governance, as illustrated in figure 1.

Additionally, the Data Controller(s) will maintain:

(a). ***The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;***

For the project overall, the name and contact details will be published on the project website as part of the *Privacy Policy* (see below). For individual use case activities, a participant information sheet will contain these details as they relate specifically to that trial. The data protection officer is defined later in section 3.8.1.

(b). ***The purpose of the processing;***

This arrangement will be documented internally and, when necessary, externally, in the relevant project deliverables. Additionally, for specific use case activities, the information leaflet will explicitly outline the purpose of the collection and processing.

(c). ***The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations***;

As (b) above.

(d). ***Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation***

This will only occur, after suitable agreement, between consortium partners and therefore governed in part by the provisions of the consortium agreement. This will also be communicated with data subjects via an information leaflet.

(e). ***Where possible, the envisaged time limits for erasure of the different categories of data***

As (b) to (c) above.

(f). ***Where possible, a general description of the technical and organisational security measures***

This will be apparent in this document (see below) and via internal project management reports.

3.5 Data Processor

In the rare scenario, where personal data is shared with project partners for development purposes, the project partner(s) would assume the role of Data Processors, as depicted in Figure 1.

However, the initial strategy for use case activities involves generating synthetic data and tests beds not integrated with customers. Because such data wouldn't be linked to any specific individual, they do not qualify as personal data and fall outside the GDPR's scope. Consequently, we do not anticipate any Data Processor activities within the project.

3.6 Data Sharing

In exceptional circumstances where real personal data may be utilized, this matter should be discussed at the General Assembly, as illustrated in Figure 1. Assurances must be established to ensure that the Data Controller can fulfil their obligations under the GDPR. This may involve drafting a non-disclosure agreement and a data sharing agreement between the partners (Data Controller and Data Processor), potentially extending the project Consortium Agreement if required.

3.7 Data Protection Impact Assessment

Article 35(1) of the GDPR states:

> *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing is **likely to result in a high risk** to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact** of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

In other words, when necessary, a Data Protection Impact Assessment (DPIA) would be performed to identify potential risks to the data subjects, and appropriate mitigation.

Prior to initiating any data processing activities, a meeting will be held with each of the use case partners. The objective of this meeting will be to conduct an initial Privacy Threshold Assessment (PTA) and ascertain whether a Data Protection Impact Assessment (DPIA) is required.

3.8 Privacy Policy

If necessity arises a TELEMETRY privacy policy will be formulated and made available on the project website. The policy is based on the Project Coordinator's own policy and those of the other partners; this policy will delineate the principles governing the collection and maintenance of personal data, particularly Project Contact Data as outlined above. This will encompass:

- The personal data that is collected;
- Why the data is collected;
- Who will have access to the data;
- What will be done with the data; and
- How long it will be retained.

The privacy policy will also include the contact details for the project Data Controller (i.e., the Project Coordinator) and the Data Protection Officer.

Any Research Data will be addressed within the individual research protocol for each use case. Typically, this sheet will reference the partner's own privacy policy, as well as the TELEMETRY policy.

Any other Data will be handled independently as part of a partner's existing privacy policy. Since no such data will be shared with other partners, there will be no link to the TELEMETRY privacy policy.

3.8.1 Data Protection Officer

Following the provisions of the GDPR Art. 37(2), the TELEMETRY project will appoint a Data Protection Officer (DPO). Apart from the specific responsibilities as laid out in GDPR Art. 39, they will:

- **be based in an EU Member State**, and is not from the Norway, UK or Ukraine partners,
- provide support to the Project Coordinator on data protection matters, including alerting them to any potential issues or changes in legislation;
- monitor any DPIA action plans; and

The project expects to appoint a DPO by month 9 of the project.

3.8.2 Publication

As a fundamental principle, there are no intentions to disclose any personal data through publication, whether in project deliverables or in conference or journal submissions. An exception might occur when the data subject(s) has provided explicit, informed, and freely-given consent within the context of a specific use case activity.

Currently, there are no plans to create or release any datasets containing personal data, even if pseudonymized or de-personalized, via any open-access repository. Any potential changes to this approach will be governed by FAIR data principles.

3.8.3 Ethics

Since we do not have direct use case participants and utilize Test-Lab environments, the Ethics topics can generally be handled by the Project Coordinator and the Use Case leads.

4 Data Use in the Project per Use-Case

In this section the use cases are outlined, the data they include and data security. The data handling of the use-cases with respect to the FAIR principles is detailed in section 5.

4.1 Aerospace Use Case

Antonov is a Ukrainian aircraft manufacturing and maintenance company with experience in the field of very large aircraft. Altogether, Antonov built about 22,000 aircraft, and thousands of Antonov aircraft are in operation in countries around the world. Thanks to the introduction of IoT technology, the collection and exchange of information between smart devices using wired and wireless networks and cloud services, it will be possible to exchange data between aircraft of various modifications and dispatch services in real time (SESAR 3 Joint Undertaking EU, Digital European Sky partnership), which contribute to the rapid adoption of the right decisions and the overall increase in the productivity of the aviation industry. This will result in more efficient flight paths, shorter take-off and landing times, and as a result, happier passengers who fly more frequently, generating more revenue for airlines.

With the advent of IoT technology, greater connectivity to individual aircraft subsystems has emerged, allowing engine manufacturers to use this data more quickly, providing faster service, as well as recommendations for operational changes, such as those that will result in fuel savings or other beneficial operations (for ex., changing the landing sequence to reduce the load on the engine).

The main goal of the use case is to identify vulnerabilities in terms of information security in the Flight Monitoring system at Antonov Company, which is being developed for automated processing of flight information transmitted from the aircraft on-line (24/7/365) in order to increase the level of flight safety, operational communication between the aircraft crew and ground personnel to increase the efficiency and profitability of commercial transportation of Antonov Company.

FLIGHT Monitoring system is an efficient tool for:

- effective management and analysis of processed flight information (parametric, voice and video information), registered by on-board flight information recording devices, during the normal operation of the aircraft fleet (An-124-100) as well as for investigations of flight accidents and incidents to people;
- 4D monitoring of aircraft flights (An-124-100).

FLIGHT Monitoring system should cover work with all flight information of the An-124-100 fleet equipped with on-board flight information recording equipment FLIGHT Monitoring, and it is designed for:

- creation of a unified information space that will allow the involved specialists to interactively receive the necessary information (parametric, voice and video) about each flight of the advanced turbo-prop aircraft, including technical characteristics on the status of the aircraft and its systems, at any time while ensuring secure personalized access for different categories of users to information;
- independent automated collection and accumulation of technical information from aircraft on hardware with its subsequent processing and distribution to certain user groups within the company's divisions;

- increasing the level of information to the specialists of the airline control center by providing operational information on the movement of the aircraft and the requested technical characteristics of the aircraft and its systems during the flight;
- providing information support to the aircraft crew during a flight or at the airfield in preparation for a flight by transferring operational data for the upcoming flight, aeronautical and other information from the control centre to the aircraft;
- operational assistance to aircraft crews and engineering and technical staff on board, in the form of recommendations for action in the event of special situations arising during the flight and/or technical operation of the aircraft outside the airline's base to eliminate defects after completed flights;
- collection and provision of accumulated information from the aircraft to the airline management in the current situation, which requires a prompt response for decision-making;
- flight safety management, taking into account the introduction of algorithms for automated processing of flight information related to the condition of aircraft equipment, monitoring compliance with aircraft operating rules by the crew in flight and engineering staff on the ground, as well as assessing the level of training of flight personnel;
- ensuring automation of risk management when planning and executing commercial flights of aircraft, taking into account the objective situation along the route and the technical condition of the aircraft, the qualifications and readiness of the crew and technical staff on board;
- ensuring automated maintenance of the "Electronic Form" of the aircraft in order to control the consumption of the actual life of the airframe and engines, as well as analyze their technical condition, quality of production and repairs.

4.1.1 Data Summary

There are different types of data, they are related to flight information (parametric, voice and video information), recorded by on-board flight recording devices, persons, objects/tools, processes, customer request.

Persons: The flight monitoring system utilizes video analytics to detect critical situations in the cargo compartment. The video stream is analyzed by the flight management system and stored at the AIS (aircraft information center). A backup is stored in a cloud-based ERP system (Awery). In order to guarantee that only authorized persons are able to start the data recording and analyzing process, an access control system is in place. Naturally the video stream could include personal data, e.g. personnel loading the cargo, thus simulated data will be used.

Order data: cargo monitoring process is initiated by an incoming customer request. This request is a data set which contains information about the customer, the cargo (including its features) he has asked to deliver, and delivery information. The original request data are created and stored in a cloud-based ERP system (Awery) and backup on the ground server.

Objects/tools: Flight data recorder and IoT equipment are used for getting initial information, personal data are not used.

Processes: all data will be analyzed by onboard monitoring system (data from IoT sensors and FDRs) and then transferred to the ground for further analysis.

4.1.2 Data Security

Participation of Antonov and creation of this use case was to improve the data security. Hence the data security will be high priority. Mechanisms to data integrity protection and risk assessment are part of the project. Additionally, no project generated data shall correlate to real persons or entities.

4.2 Smart Manufacturing Use Case

The Smart Manufacturing use case of the TELEMETRY project is based on Nokia's Factory-in-a-Box (FiaB) solution. This solution serves several purposes:

- It is an innovation and research environment to explore new ideas, which might be relevant to evolve the digitization of Nokia's end-to-end supply chain.
- It is a proof of concept and feasibility study for implementing entire production environments in small mobile units.
- It is a showcase for Nokia's product portfolio and offerings towards the industrial sector for the upcoming 5G based networking revolution.

The FiaB in TELEMETRY focuses more on the SW stack of smart manufacturing and Industry 4.0 aspects than on the physical production process.

4.2.1 Data Summary

In the FiaB - as in all industrial environments - there are different types of data, they relate to persons, objects/tools, processes, Identity and Access Management (IAM), customer request, order data.

- **Persons**: The FiaB utilizes video analytics-based worker safety tools. The video stream is analysed in the FiaB to detect critical situations. The live video stream is being forwarded to a machine learning application, which scans the stream for workers without proper security gear. The result (number of people found, number of people without security gear) is being forwarded to a health&safety application, which establishes the appropriate actions based on the findings. The video stream is not recorded or stored; it is only used to analyze the above situation in real time.
- **IAM**: The cellular network in the FiaB uses SIM-cards for access control. All SIM-card data are stored locally in the FiaB. There are no SIM-cards issued to persons, only to tools and computers in the FiaB. There are passwords to access the software entities in the FiaB from remote and within the FiaB.
- **Order data**: A production process is initiated by an incoming customer order. This order is a data set which contains information about the customer, the objects (including its features) he has ordered, and delivery information. The original order data are created and stored in a cloud-based ERP (Enterprise Resource Planning) and MES (Manufacturing Execution System) tool.
- **Objects/tools**: Most of the tools have SW based control systems and operate on data, which describe the object to be produced. In addition, most tools, i.e. HW, create operational data during run time, e.g. power consumption, frequencies, temperatures, utilization, etc.
- **Processes**: As a central part of FiaB's smart manufacturing implementation a semantic data hub is used, where all data are semantically modelled, accessible, and where derived data are being stored.

4.2.2 Data Security

Since the FiaB is an innovation and test environment, any person, product, or customer related data are experimental data. There is no correlation to real persons of production orders of Nokia's manufacturing facilities and supply chain.

Wherever personal data is being processed, or images taken from persons, this happens with the consent of the person, including the agreement of these data to be processed by the SW components employed in the smart factory use case. See Annex for a template.

4.3 Telecommunications Use Case

The TELCO use case (UC3) will evaluate the TELEMETRY tools in the Home Gateway (our Device Under Test or DUT) context with a testbed simulating a real environment where Home Gateways are placed at the border between the Telco networks and the customer's devices such as PC, Smartphone, IPTV, Cameras and so on. The DUT will be interconnected from one side to the internal Local Area Network (reproducing the home context) and from the other side to the external environments, the public Internet and the interconnection to the other partners' labs via secure VPNs. The main objectives of the Telco test bed are the following:

- Reproduce the real target network environment (i.e. residential customer scenarios);
- Permit the remote access to the DUT from the tool owner to the partners.
- Deploy real Home Gateway devices actually used by Telecom Italia for their residential customers to be used to validate the TELEMETRY testing tools. This will happen in a Telecom Italia test environment.
- Provide an isolated environment where it is possible replicate realistic network IP traffic by means of traffic generators.
- Host tools (HW/SW) needed by the tool owners to perform the security tests or host specific sensors/probes.
- Provide separated environments for different tool owners when needed.
- Protect the testing environments from unauthorized access by means of firewalls and secure VPNs.

4.3.1 Data Summary

In the Telco environments no real data will be managed. Synthetic data of different types will be used. Such data simulate real data related to persons, tools, Identity and Access Management (IAM).

- **Persons**: The Home Gateway manages the IP traffic generated by the different services used by the customers, including their family or friends. Although such services are usually encrypted, the IP traffic can still be used to gather information for profiling the customer. Anyway, such traffic will be only synthetic.
- **IAM**: The RGW can be accessed directly by an administrator via SSH or the Web interface (HTTPs) by means of login/password. Usually, no other user can be defined. Moreover, the environment will manage the credentials used by the project partners to access the LAB from remote site via secure VPN.
- **Tools**: In the test bed will be installed several tools (HW/SW) used to reach the aim of the project. Such tools will collect and generate other information related e.g., to power consumption, temperatures, CPU/RAM utilization, anomalous events, etc.

4.3.2 Data Security

The remote access to the UC3 lab will be protected by 2-faktor authentication and using an encrypted channel. Additional any person, product, or customer related data are experimental data. There is no correlation to real persons or customers. Thus, data security requirements relate to the commercial interest of the project partners.

5 FAIR

Whereas no real data from natural persons is collected in the use cases, other data is being generated, e.g. the SSM knowledge base, possibly SBOM data. Some of the data is not yet known and will be added to the DMP at a later update.

In general, TELEMETRY caters for the FAIR principle by providing detailed metadata for each dataset to enhance findability. Storing data in accessible repositories with clear access instructions. We ensure ease of access while maintaining necessary security measures. Standardized formats are adopted and collaborating between the different partners with their unique toolset promotes interoperability and facilitates seamless integration across platforms.

Additionally, clear licensing terms, where data can be made available, and comprehensive documentation on data quality and processing steps promote reusability and encourage broader scientific engagement and impact. By implementing these strategies, TELEMETRY maximizes the value of its data assets.

5.1 Making data findable, including provisions for metadata

There are different entities, categories and concepts within TELEMETRY. From an almost closed system of the airplane in UC1, over the versatile Factory in the Box in UC2, to a Telecommunications home gateway in UC3. Especially in UC3, but also in the other use cases the data origin, and thus data subject, is of different types. Adding the right metadata and identifiers supports creation of better data sets and findability.

5.1.1 UC 1 Aerospace specifics

Data in the aerospace use case, originating from the flight recorder and enhanced with sensor data, by its nature will be very structured data. Metadata and good documentation will be added, where appropriate. Additionally, the data like the risk report and software bill of material (SBOM) also requires having components and data originating from those being identifiable.

5.1.2 UC 2 Smart Manufacturing specifics

Most of the data which will be used in the project, i.e. which will be protected and added with metadata through the concept of the TELEMETRY project. Additionally, the project tests out industrial data space based technology for facilitating finding of data.

All data are solely created for the purpose of the TELEMETRY project, they do not resemble or are not derived from Nokia's production processes.

IAM data, which has special GDPR protection, will not be created and thus is not accessible after the end of the project.

5.1.3 UC 3 Telecomm specifics

Most of the data which will be used in the project, i.e. which will be protected through the concept of the TELEMETRY project, are added with meta-data. Additionally, blockchain based ledger technology may be tested to facilitate finding and protection of data. All data are solely

created for the purpose of the TELEMETRY project, they do not resemble or are not derived from TIM's production processes.

No GDPR relevant data are available and can be accessed after the end of the project. All data will be deleted by following a secure disposal process.

5.2 Making data openly accessible

GDPR predominantly emphasizes safeguarding data protection and privacy rights, whereas the FAIR data principles prioritize improving the usability and efficacy of data sharing and management. TELEMETRY will harmonize its data management practices with both sets of standards by integrating privacy safeguards into data sharing protocols, maintaining transparency regarding data usage, and adopting secure and standardized data handling procedures. Although GDPR-relevant data isn't anticipated, if required, tailored measures like pseudonymization procedures or specialized analyses involving the Security Advisory Board will be implemented.

5.2.1 UC 1 specifics

Most of the data which will be used in the project, i.e. which will be protected through the concept of the TELEMETRY project are available for all members of consortium and can be released to public use after prior approval from Antonov. Especially data from the cargo monitoring system that can be sensitive as related with transportation of the cargo under Aerospace programs, and usually customers expect their data to be treated confidentially and not being shared.

5.2.2 UC 2 specifics

In UC2, we will explore how anomalies in the operation of a factory robot can be detected by machine learning. Such anomalies may arise from typical degradation over time or deliberate interference by malicious entities seeking to disrupt the production workflow, thereby inducing substandard product output or machinery malfunction.

The training data, along with the associated metadata, for the machine learning models will be made available after the project is completed.

5.2.3 UC 3 specifics

The data traffic and configuration files utilized in establishing the testing environment for evaluating the TELEMETRY framework in security testing will be produced using dedicated data traffic generators and standard configuration files not related to real-person information. This data will be stored and, when necessary, shared in standard formats such as .PCAP files or XML/JSON files.

5.3 Making data interoperable

Adoption of standardized formats is the best way to make data interoperable. Additionally, documentation on the collection and creation of data sets allow later users to understand particularities that might arise when analyzing the data.

5.3.1 UC 1 specifics

All the data used in the Aerospace use case will be structured and exchanged by using standard protocols (IP protocols) and data format Metadata standards: ARINC429 [6], ARINC717 [7], IRIDIUM [8].

5.3.2 UC 2 specifics

A guiding principle when implementing the FiaB concept is to use as much as possible standard formats and definitions, e.g. CSV files for analytics, W3C definitions for semantic web, etc.

In addition, the work packages will define which standards will be used for metadata creation for the policy descriptions and the risk analysis.

5.3.3 UC 3 specifics

All the data used in the Telco use case will be structured and exchanged by using standard protocols (IP protocols) and data format (e.g. JSON, XML, etc.).

5.4 Increase data re-use

Data re-use is set boundaries by the purpose-driven data use mandated by the GDPR. And a balance between commercial and macro-social interests. With the use of IP protection law, commercial interest can be catered for, while then the maximal re-use can be aimed for.

The common project approach will be that besides the reuse of actual data, the re-use of architecture, lab-setup-description and interchangeable formats will be an element that TELEMETRY delivers to increase data re-use. In the further course of the project, we will try to identify or create data-sets that can be provided to the public.

5.4.1 UC 1 specifics

Due to the nature of the setting in which the data is being collected, UC1 being the closest use case to real-life-commercial activity, the data re-use will be dominantly internally. It will be discussed in the project if we can find data to be opened for re-use.

5.4.2 UC 2 specifics

Nokia will follow the within the project agreed upon approach, while protecting the IP of the tool and component suppliers.

5.4.3 UC 3 specifics

TIM will follow the within the project agreed upon approach, while protecting the IP of the tool and component suppliers.

6 Scientific Publications

TELEMETRY's results and accomplishments will be disseminated within the scientific community, industry, and other pertinent stakeholders. Open access will be prioritized for all publications, including peer-reviewed scientific publications, to the fullest extent possible.

Authors of such publications will select the most suitable means of sharing their findings, with these publications being archived in an open-access repository both during and after the project's duration.

In order to maximize budget efficiency, TELEMETRY will primarily employ a "green open access" approach whenever feasible, ensuring immediate availability of results in accordance with publisher policies. In instances where timely open access dissemination cannot be achieved through "green open access" and "gold open access" is an option, TELEMETRY will opt for "gold open access". More information about the open access rules can be found at https://open-access.network/en/information/open-access-primers/green-and-gold

In addition, all scientific publications will be deposited in a trusted and OpenAIRE compliant repository (Zenodo.org)

7 Conclusions

In this document the handling of the data within the project TELEMETRY was described. The deliverable covers the different definitions of data management and their use in the three use cases. Also, aspects of how publications are handled and the devotion to open access have been described.

8 References

[1] Robert Seidl, Jörg Abendroth (Nokia), Norbert Götze, 2024, TELEMETRY D6.1 Project Handbook and Quality Assurance Plan
[2] EFTA, checked 21.2.2024, https://www.efta.int/Legal-Text/EEA-Agreement-1327
[3] European Data Protection Supervisor (EDPS), checked 21.2.2024, https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en
[4] Draft Law (in Ukrainian), checked 21.2.2024, https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF
[5] Second Draft Law (in Ukrainian) https://itd.rada.gov.ua/billInfo/Bills/Card/40707
[6] Aeronautical Radio INC.: Mark 33 digital information transfer system (DITS), May 2004. http://www.bosch-semiconductors.de/media/ubk. ARINC specification 429 part 1-17
[7] Aeronautical Radio INC.: ARINC717-15,2011, Flight Data Acquisition and Recording System
[8] MANUAL FOR ICAO AERONAUTICAL MOBILE SATELLITE (ROUTE) SERVICE Part 2-IRIDIUM Draft v4.0, 2007, checked archived version at 20.2.2024, https://web.archive.org/web/20140222201753/http://legacy.icao.int/anb/panels/acp/wg/m/iridium_swg/ird-08/ird-swg08-ip05%20-%20ams(r)s%20manual%20part%20ii%20v4.0.pdf

9 Annexes

Template for consent form if there are visitors to the experiment lab.

TelemetryConsentFormTemplate.docx