IoT Week 2022

Cross-domain data usability in IoT ecosystems comprising IoT devices, humans and machines

Michelle Wetterwald

14/10/2022

Outline

- Motivation
- Short presentation of STF601
- Use cases analysed
- Service and operational requirements
- Conclusion

Motivation

- **Usability of the data and services that the IoT devices and platforms deliver** was a key issue not yet addressed (see STF 505 TR 103 376 and AIOTI Gaps report Release 2 published in Jan 2020)
- **In addition to user experience (ergonomics) or the accessibility of the ICT equipment**, the usability topic should also be considered from a data and service point of view, i.e. usability of the data and services that the IoT devices and platforms deliver
- This work **complements other AI activities at TC SmartM2M** , including the evaluation of **opportunities for improving AI systems performance through the use of oneM2M**
- Standardizing the usability of data and services from IoT devices and platforms may have a **strong impact on big data and AI technologies**.
  - Making use of AI for **knowledge presentation and management** (organization and visualization) for both **machines and humans**
  - Improving **configuration and management tasks at IoT devices and platforms** to increase the reliability of the data used by AI

STF601 Project Description

- **Title** : Cross-domain data usability of IoT devices for humans and machines
- **Objective** : Cover a missing key link of the IoT eco-system chain: standardization of usability of the data and services that the IoT devices and platforms deliver
  - in complement to user experience (ergonomics) or the accessibility of the ICT equipment which are already covered by other groups
- **Time schedule:** started Feb 3, 2021 - closed July 11, 2022
- **Experts**

Expert	Organisation
Michelle Wetterwald	Netellany SASU (STF Leader)
Mauro Dragoni	Fondazione Bruno Kessler
Bob Flynn	Exacta Global Smart Solutions
Jumoke Olumide	EX2 Management

- **STF web page** at: https://portal.etsi.org/STF/stfs/STFHomePages/STF601
- **Reporting Committee** : ETSI TC SmartM2M (STF funded by ETSI)
- **Other committees consulted** : oneM2M RDM, AIOTI WG03, ETSI TC HF, TC SmartBAN, EP eHEALTH, ISG E4P, 3GPP SA1, SC USER, ISG ENI, TC CYBER, TC ITS, TC ATTM, ISG OEU

Deliverables

- **TR 103 778** “Use cases for cross-domain data usability of IoT devices”, 20.12.2021
  - To identify, select and describe use cases where the IoT data and services require data usability specifications
  - To analyze the impact of these use cases for both machines and humans
  - https://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf
- **TS 103 779** “Requirements and Guidelines for cross-domain data usability of IoT devices”, 19.05.2022
  - To define minimum requirements for data and services data usability on professional and general public IoT devices and platforms, whether they are critical or not
  - To develop a horizontal cross-domain specification encompassing these requirements
  - https://www.etsi.org/deliver/etsi_ts/103700_103799/103779/01.01.01_60/ts_103779v010101p.pdf

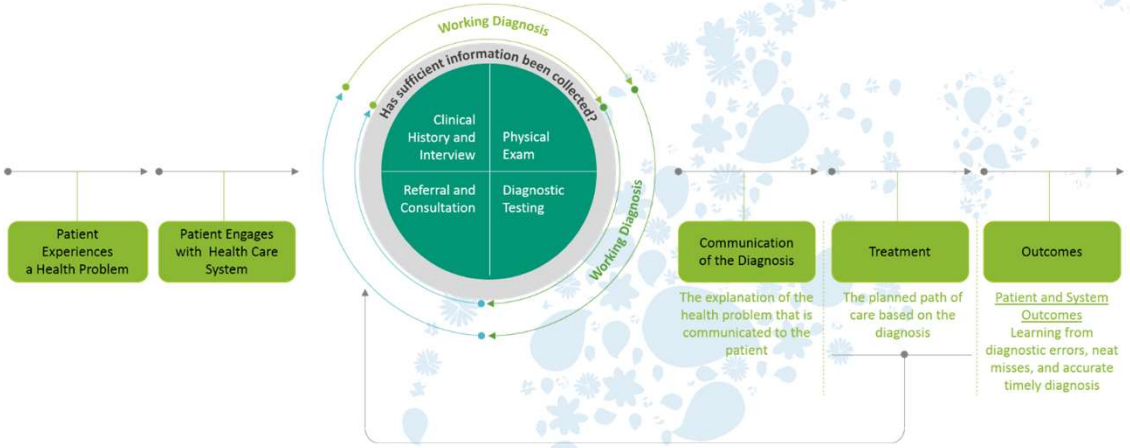
Use cases description & analysis (TR 103 778)

- A collection of **33 use cases** covering the following **12 domains**:
  - Healthcare; Public and Emergency services; Industry and manufacturing; ICT networks management; Agriculture and farming; Mobility (transportation); Energy; Building; Retail; Large events; Smart lifts; and Smart Cities.
- Use case template aligned with **the template used by oneM2M**
- **Analysis** of each of the use cases
  - Characterize **actors** that are Machine or Human
  - Identify **Data consumer**
  - Identify how invalid "data" can "**compromise data usability**"
- **Summary table** of the conclusion per use case

Use Case #	Use Case	Data Owner	Data that may be compromised	Consequence	Impact of Failure (H/M/L)	Recommendation	Residual Impact after Recommendation
A3	Diagnostic eHealth	Physicians, Patients, Healthcare Organizations, AI engine.	Information provided by clinicians. Information provided by patients. Device and IoT data (when used).	The AI-based diagnostic process implies the aggregation of information coming from clinicians, patients, and sensors (when used). If at least one of this type of information is not managed properly by the related actor, the overall data usability may be compromised since the AI system would not be able to run the diagnosis discovery engine properly.	H	Recommendations related to A2 are all inherited. [9] If third-party services are used for performing specific classification activities, these services have to described within the system by annotating generated information with service metadata in order to support traceability.	The application of these recommendations may reduce the risk to L.

Use case example: A.3 - Diagnostic eHealth

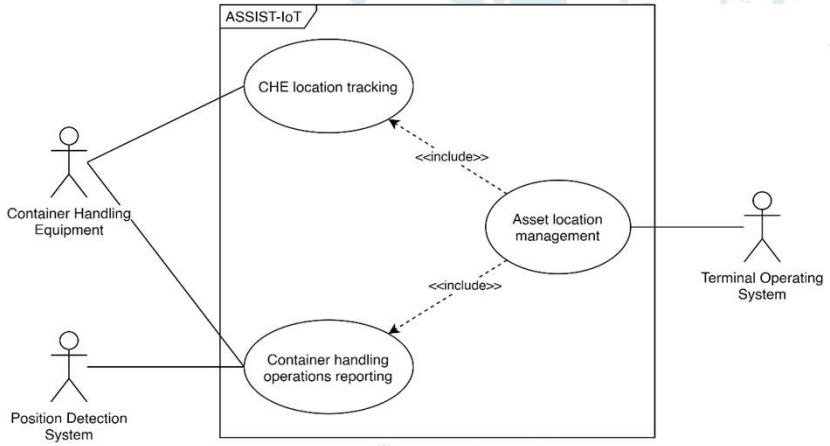
- This case addresses the challenge of **monitoring diagnostic sensors** that are in charge of delivering measured values taken at a certain time within a given context from a specific patient to its clinician
- Actors: ***[Humans]:*** Physicians, Patients; ***[Organization]:*** Healthcare Organizations; ***[Machine]:*** AI engine
- Data that may compromise data usability:
  - information **provided by clinicians**,
  - information **provided by patients**,
  - **device and IoT data**



- Conclusion: The **AI-based diagnostic process** implies the **aggregation** of above information. If at least one of this type of information is **not managed properly** by the related actor, the overall data usability may be compromised since the **AI system would not be able to run the diagnosis discovery engine properly**.

Use case example: F.3 - Port automation: Tracking assets in terminal yard

- In a port, containers are managed by heavy machinery equipment (cranes). The main challenge to solve is to **enable traceability of containers within the port terminal** to avoid losing them, and to **enhance the operational efficiency** of terminal operators (including internal and external drivers).
- Actors: ***[Humans]:*** Terminal manager, Container Handling Equipment (CHE) drivers; ***[Machine]:*** Terminal Operating System (TOS); ***[Devices]***: CHEs, CHE Position Detection System (PDS)
- Data that may compromise data usability:
  - **Identification and location** of CHEs and containers ,
  - **Identification of other devices** within the terminal yard,
  - Information about **operation on containers**
  - **Timestamp** and location of where the container is picked up and placed



- **Conclusion**: Location management, data synchronization, geolocation precision, objects identification
  - Lack of data usability may result in the **loss of containers**, which has mainly **economic consequences**

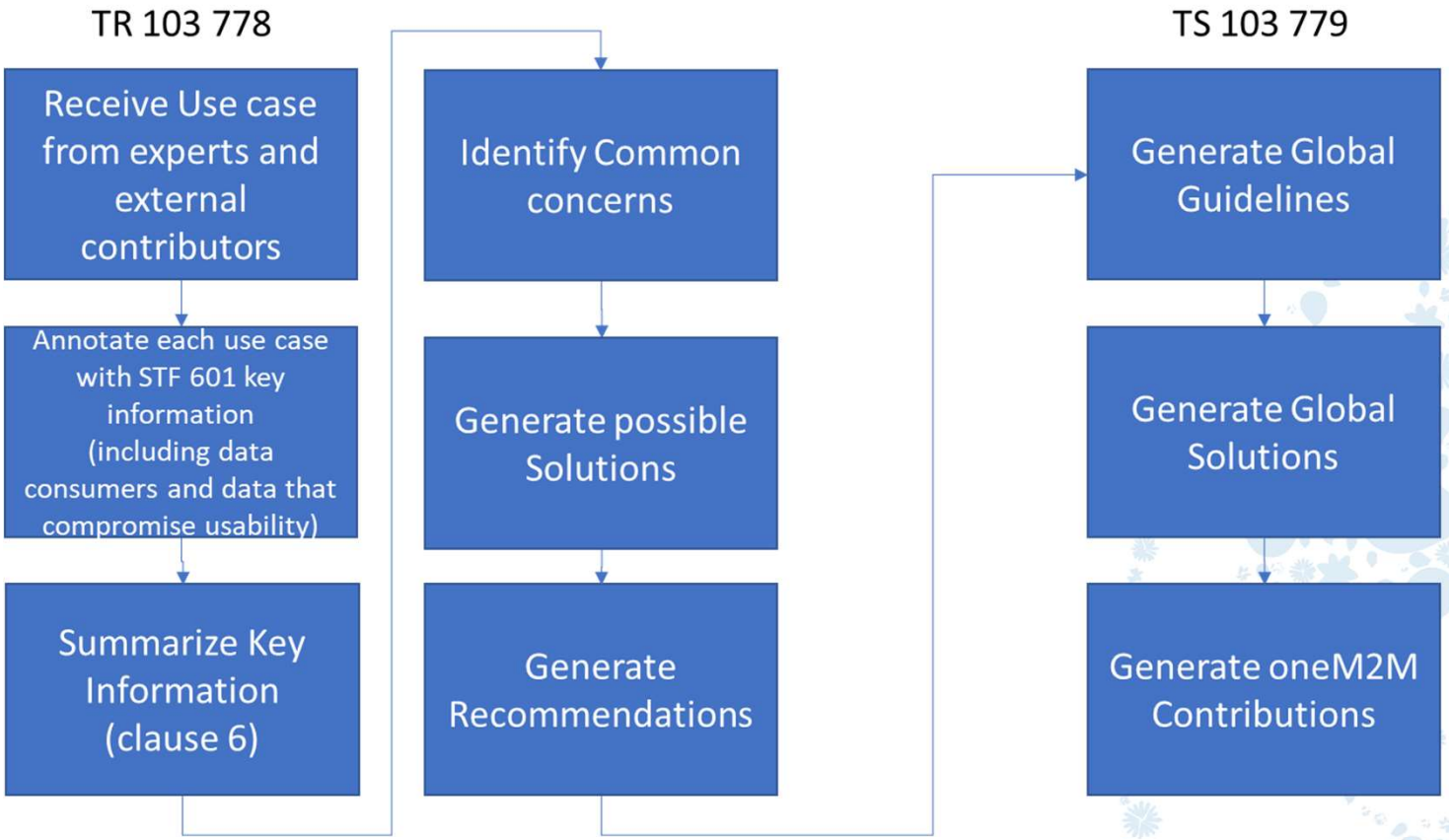
This use case has been contributed by the ASSIST-IoT project.

Use cases analysis

- Conclusion : **list of recommendations**, classified under the following topics: **setup, configuration, ML output, IoT system operation and privacy and security**.

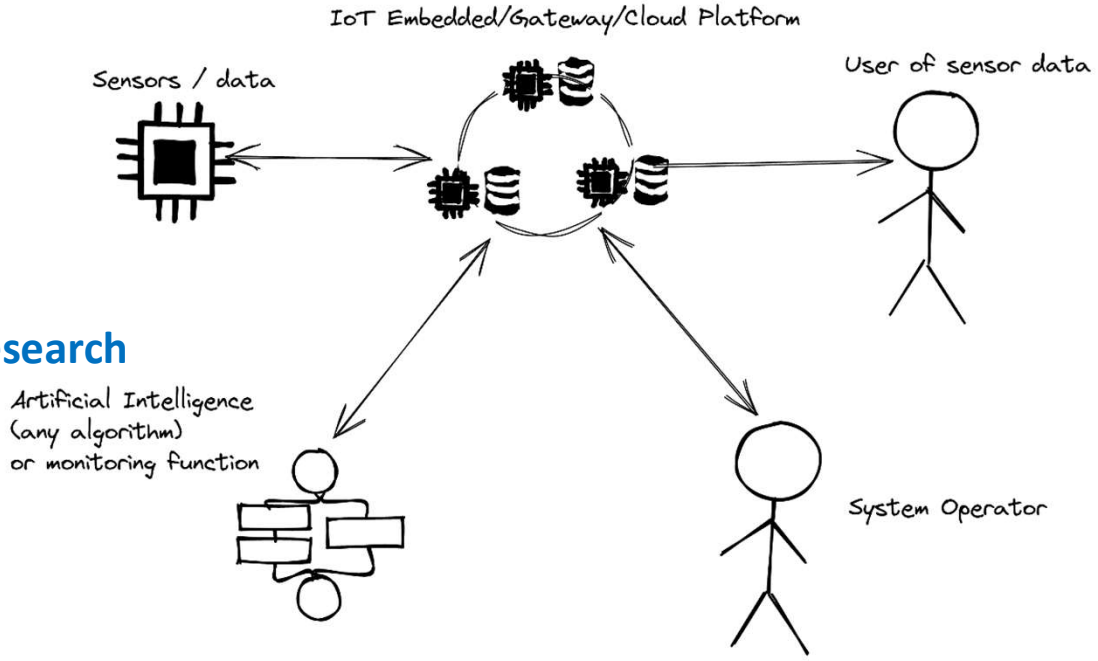
Category	Description
Setup	Easy way for sensor data to be directed to a user (human or ML algorithm).
Setup	describe data format such that it can be used without ambiguity by its intended user (human or ML algorithm).
Configuration	transform data, if necessary, for a ML algorithm input or human user installation
Configuration	describe the sensor data quality, or suitability to use in different scenarios
ML output	capture classification of ML algorithms along with the data of interest that generated the classification
ML output	terms used for output: ontology for ML results.
ML output	organize output in a manner that is easy to find and understand "important" data without any ambiguity.
ML output	data duplication should be avoided, if possible, e.g. image from a camera is provided. Then it is "analysed" by an ML algorithm. A classification is determined. The image and classification are stored again (based on #7) but this should be avoided as it will create multiple instances of the same data (raw image) Just store the "classifications".
ML output	identify the ML module used to provide a classification (traceability).
IoT system operation	timestamp and geolocate the data when necessary
IoT system operation	ensure that data accessibility is enabled to all authorized users.
IoT system operation	ensure that data interoperability is enabled if data should be shared between different IoT systems.
IoT system operation	ensure that the system is properly maintained and default components can be easily identified.
Privacy and security	protect against privacy, security and data integrity breaches

Process to prepare the requirements



Service and operational requirements

- **Requirements and guidelines** for preserving data usability
  - **Service requirements**
  - **Operational requirements**
  - **To be fulfilled by**:
    - Sensor/data sources
    - IoT Platform
    - AI/ML or monitoring function
    - Operator of system
    - Data users
- Annex A: In-depth **analysis and summary of research literature** that were related to these topics
  - Interoperability
  - Collecting data from sensors
  - Granularity
  - Traceability



Example: Operational requirements to be fulfilled by operator of system

Requirement number	Related recommendation	Requirement
REQ_OPE_4_001	IoT infrastructure/devices bootstrap.	At the time of deployment, operators shall verify that the overall infrastructure works properly and that all components are able to communicate each other.
REQ_OPE_4_002	IoT infrastructure/devices bootstrap.	At the time of deployment, operators shall verify that all human target users are able to receive required data from the system.
REQ_OPE_4_003	IoT infrastructure/devices bootstrap.	At the time of deployment, operators shall verify that all artificial intelligence components are able to receive required data from the system.
REQ_OPE_4_004	Maintenance of IoT infrastructure/devices.	Maintenance shall be performed periodically to verify the proper operation of the system and prevent failure of the devices and sensors. All issues found during the verification process shall be resolved.
REQ_OPE_4_005	IoT data interoperability.	At the time of deployment, operators shall verify that the format of the IoT platform data is understandable by any external device or human expected to consume them.
REQ_OPE_4_006	Preservation of integrity, privacy and security.	All data consumers who may need to access them shall be granted authorized access to the IoT platform data.
REQ_OPE_4_007	Data format description and intelligibility	The deployed system should be scalable, accepting inputs from all sorts of sensors if relevant.
REQ_OPE_4_008	Data format description and intelligibility.	Object identification should be setup and configured properly to prevent mishandling of objects by the IoT platform.
REQ_OPE_4_009	Data coordinates.	Data from all object sources should be synchronized (e.g. identical time reference).
REQ_OPE_4_010	Preservation of integrity, privacy and security	Privacy of personal data should be ensured for the IoT platform user and all affected humans (see also ETSI EN 303 645 [2]).
REQ_OPE_4_011	Preservation of integrity, privacy and security	The data flow for safety applications shall be secured (see also ETSI EN 303 645 [2]).

Conclusion

- Objective
  - Cover a missing key link of the IoT eco-system chain: **standardization of usability of the data and services that the IoT devices and platforms deliver**, in complement to user experience (ergonomics) or the accessibility of the ICT equipment which are already covered by other committees.
- External committees contacted
  - **oneM2M RDM, AIOTI WG Standardization, ETSI TC HF**, TC SmartBAN, EP eHEALTH, ISG E4P, 3GPP SA1, SC USER, ISG ENI, TC CYBER, TC ITS, TC ATTM, ISG OEU
- Use cases (TR 103 778)
  - analysis of **33 use cases** from real life scenarios in **12 different vertical domains** were analyzed focusing on data consumers and **which data could be compromised in the system**
  - consequences and impact of data not being usable in each of these scenarios and how to address the risk
- Requirements (TS 103 779)
  - measures to **ensure data usability from a generic point** of view across all these domains (horizontal requirements)
  - both **service and operational requirements** that different elements in an IoT system need to fulfil
- Follow-up
  - Feed **oneM2M RDM (TR-0068)** with selected use cases and requirements **to enable supporting AI capabilities**

Any further questions?

Michelle Wetterwald

NETELLANY / FBConsulting

Sophia Antipolis, France

Email: michelle.wetterwald@netellany.fr