|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | RDM 54 |
| Source:\* | Bob Flynn (Exacta GSS); bob.flynn@exactagss.com |
| Date:\* |  |
| Reason for Change/s:\* | Add recommendations from STF601 relevant to AI enhancements |
| CR against: Release\* | Rel-5 |
| CR against: WI\* | Active <WI-xxxx>  MNT maintenance / < Work Item number(optional)>  Is this a mirror CR? Yes  No  mirror CR number: (Note to Rapporteur - use latest agreed revision)  STE Small Technical Enhancements / < Work Item number (optional)>  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TR-0068 v0.4.0 |
| Clauses \* | Annex A |
| Type of change: \* | Editorial change  Bug Fix or Correction  Change to existing feature or functionality  New feature or functionality  Only ONE of the above shall be ticked |
| Other TS/TR(s) impacted | None |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES  NO  This CR may break backwards compatibility with the last approved version of the TS? YES  NO |
| Template Version: January 2019 (do not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

# Introduction

STF 601 has delivered TS 103 779. For a full summary for STF 601 please refer to TP-2022-0028-STF601\_Data\_Usability.

This contribution is intended to contribute for consideration the recommendations and guidelines from TS 103 779 that apply to WI-0105 and the oneM2M Service Layer platform.

This contribution include those recommendations that can be applied to the oneM2M service layer or recommendations that can be included in some form in other types of documents, for example sensor requirements might be captured in a developer guide as an example of how a sensor device is created.

The proposed approach is to include all of the requirements in the annex and then add two columns

1. Meets requirements -> YES, NO, NA (not applicable)
2. Remarks ->
   1. Yes: remarks include notes about “how” it is met
   2. No: remarks include notes about plans, if any, to address
   3. NA: remarks include why this is out of scope

### -----------------------Start of change 1-------------------------------------------

## A.4 ETSI TR 103 799 Requirements and Guideline

This list of requirements are extracted from ETSI TS 103 779. The table includes an assessment of whether oneM2M has the ability to meet those requirements, whether there are future plans to meet the requirements or whether the requirements are not applicable to the oneM2M specifications.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Requirement number | Related recommendation | Requirement | Meet  Reqt | Remarks |
| REQ\_SERV\_1\_001 | Terminology. | Data generated or provided by a sensor shall have a description of the data using a shared terminology defined within an ontology. | Yes | Data sources can provide a description of data using <semanticDescriptor> resources.  TBD: What are good ontologies to describe data? Should oneM2M have requirements or recommendations? |
| REQ\_SERV\_1\_002 | Mitigation of data heterogeneity. | A data mitigation procedure should have foreseen if sensors generating data are provided by different manufacturers. Pre-processing of raw data from sensors to a format required by a ML algorithm may be a sufficient mitigation. |  |  |
| REQ\_SERV\_1\_003 | Data format description and intelligibility. | Data generated or provided by a sensor should have a description of the format used for generating or providing such data. |  |  |
| REQ\_SERV\_1\_004 | Data quality. | Data generated or provided by a sensor shall have a description of the granularity (in terms of numerical precision, if any, and frequency) adopted for generating or providing such data. |  |  |
| REQ\_SERV\_1\_005 | IoT infrastructure/devices bootstrap. | The sensor data shall be available to their consumer (human or machine algorithm). |  |  |
| REQ\_SERV\_1\_006 | Data quality. | The sensor data confidence level should be known to enable proper processing by the data consumers. For example, a temperature sensor may provide meta-data describing the accuracy of the measurement from the device. |  |  |
| REQ\_SERV\_1\_007 | Data quality. | A sensor / data source shall be able to report potential failure conditions (low battery, etc.). |  |  |
| REQ\_SERV\_2\_001 | Data format description and intelligibility. | If historical data is available the IoT platform shall allow download of data in a bulk format such as CSV, Apache Parquet, or other formats. |  |  |
| REQ\_SERV\_2\_002 | Terminology. | IoT platform shall allow linking of data to a semantic definition of the data. |  |  |
| REQ\_SERV\_2\_003 | Traceability. | IoT Platform shall support discovery of services or algorithms to process data coming from IoT data sources (e.g., sensors). |  |  |
| REQ\_SERV\_2\_004 | Data format description and intelligibility. | Data from the IoT platform shall be easily understandable for a data consumer monitoring the platform |  |  |
| REQ\_SERV\_2\_005 | Data format description and intelligibility. | Data presentation and integrity from an IoT platform shall ensure a valid algorithm / AI decision. |  |  |
| REQ\_SERV\_2\_006 | Mitigation of data heterogeneity. | Data from different sources shall be transformed and/or aggregated, as necessary, to fit into the ML algorithm and enable scalability. |  |  |
| REQ\_SERV\_2\_007 | Data quality. | The IoT platform shall be designed in a scalable manner as a large number of objects may need to be tracked reliably with position, identification, and timestamp. |  |  |
| REQ\_SERV\_2\_008 | Traceability | Each data shall be uniquely identifiable. In cases where ML algorithms generate a copy of data, a reference to the original source should be available as well. |  |  |
| REQ\_SERV\_3\_001 | Explainability. | Used machine learning algorithms shall be transparent and to provide explanations about the output produced. An appropriate ontology or semantics should be used. |  |  |
| REQ\_SERV\_3\_002 | Data format description and intelligibility. | Used artificial intelligence components shall provide a description of the features received as input. An appropriate ontology or semantics should be used. |  |  |
| REQ\_SERV\_3\_003 | Data format description and intelligibility. | Used artificial intelligence components shall provide the list of the data formats that they are able to read. For example: “Component X shall receive as input a list of natural language sentences already tokenized.”, or, “Component Y shall receive as input a set of 24 numbers in double precision in the race [0,1].”. When needed, an appropriate ontology or semantics should be used. |  |  |
| REQ\_SERV\_3\_004 | Data format description and intelligibility. | Used artificial intelligence components shall provide a description of the format provided as output. An appropriate ontology or semantics should be used. |  |  |
| REQ\_SERV\_3\_005 | Terminology.  Output management. | The content of the report produced by exploiting the output of the ML algorithm should be comprehensive and unambiguous to enable proper operation of the IoT system. |  |  |
| REQ\_SERV\_3\_006 | Output management. | The events generated by the platform shall be easy to understand without ambiguity by the system operator. |  |  |
| REQ\_SERV\_3\_007 | Preservation of integrity, privacy and security. | Monitoring components shall not be able to access data instances for which they are not granted authorization. |  |  |
| REQ\_SERV\_3\_008 | Output management. | The algorithm output should be able to highlight important data. |  |  |
| REQ\_SERV\_4\_001 | Preservation of integrity, privacy and security. | The operators shall verify that the system is compliant with the regulations related to data privacy. |  |  |
| REQ\_SERV\_4\_002 | Preservation of integrity, privacy and security. | The operators shall verify that the system is compliant with regulations related to the ethical management of data. |  |  |
| REQ\_SERV\_4\_003 | Preservation of integrity, privacy and security. | The operators shall verify that the infrastructure does not present data integrity breaches. |  |  |
| REQ\_SERV\_4\_004 | Preservation of integrity, privacy and security. | Procedures for the management and resolution of possible data-related issues shall be defined. |  |  |
| REQ\_SERV\_5\_001 | Output management. | Users should have the knowledge to access the outcome of the artificial intelligence components. |  |  |
| REQ\_SERV\_5\_002 | Data format description and intelligibility. | Users shall be equipped with tools able to read properly the data format with which outputs are produced. |  |  |
| REQ\_OPE\_1\_001 | Data coordinates. | The data measured by the sensors shall be time-stamped. This will allow to evaluate a potential repetition rate or data redundancy / duplication. |  |  |
| REQ\_OPE\_1\_002 | Data quality. | When relevant, the geolocation measurement/ configuration of the remote sensors shall be reliable. |  |  |
| REQ\_OPE\_1\_003 | Data quality | The accuracy of the measurement results (quality of sensor data) shall be expressed as a percentage. |  |  |
| REQ\_OPE\_1\_004 | Maintenance of IoT infrastructure/devices. | The data consumer shall be able to reset the condition that led to an alert or to maintenance once it has been processed. |  |  |
| REQ\_OPE\_1\_005 | Maintenance of IoT infrastructure/devices | When relevant (i.e. depending on its functional objective), a sensor / data source shall support remote maintenance (software updates, battery and function check, etc.). |  |  |
| REQ\_OPE\_2\_001 | Output management. | Key metrics (latency, throughput, memory usage, processor utilization, disk space, resource capabilities (CPU and memory speed), temperature) should be defined and provisioned. |  |  |
| REQ\_OPE\_2\_002 | Data coordinates. | All data handled by the IoT platform should be properly timestamped and geolocated when relevant, to ensure traceability of the subsequent processing. |  |  |
| REQ\_OPE\_2\_003 | Data access. | Data from the IoT platform should shall be easily available to an authorized data consumer accessing from an external device. |  |  |
| REQ\_OPE\_2\_004 | IoT data interoperability. | The platform shall be able to propagate any data change to all components easily. |  |  |
| REQ\_OPE\_2\_005 | Maintenance of IoT infrastructure/devices. | The data consumer shall be able to understand how to act on the IoT platform to check the validity of data delivered by sensors (e.g. to identify faulty devices and sensors). |  |  |
| REQ\_OPE\_2\_006 | Maintenance of IoT infrastructure/devices. | The IoT platform operator shall have the means to enable/disable the communication and service features of any data source or sensor. |  |  |
| REQ\_OPE\_2\_007 | Data quality. | The data from an IoT platform should be accurate and reliable. Deployment of redundant sensors/IoT devices could enhance the reliability of the data. AI and fusion of data from multiple sensors could help to guarantee the validity of the data produced by the platform. |  |  |
| REQ\_OPE\_3\_001 | Data quality. | Used machine learning/monitoring algorithms shall verify the integrity of the data received as input. |  |  |
| REQ\_OPE\_3\_002 | Mitigation of data heterogeneity. | Used machine learning/monitoring algorithms shall verify the format of the data received as input. |  |  |
| REQ\_OPE\_3\_003 | Output management. | Used machine learning algorithms shall communicate the output of the data processing operations. |  |  |
| REQ\_OPE\_3\_004 | Maintenance of IoT infrastructure/devices. | Monitoring components shall alert in the case that new data are not provided. |  |  |
| REQ\_OPE\_3\_005 | Maintenance of IoT infrastructure/devices. | Monitoring components shall alert in the case that undesired events are detected. |  |  |
| REQ\_OPE\_3\_006 | Maintenance of IoT infrastructure/devices. | Monitoring components shall verify the persistency of the connection with data sources. |  |  |
| REQ\_OPE\_3\_007 | Data duplication. | Used machine learning algorithms shall mitigate data duplication issues to avoid biases during training operations. |  |  |
| REQ\_OPE\_3\_008 | Explainability. | Used machine learning algorithms shall provide the description of the semantic meaning of input characteristics. |  |  |
| REQ\_OPE\_3\_009 | Explainability. | Used machine learning algorithms shall provide a description concerning the motivations for which a specific classification has been provided by the platform with respect to the input features. |  |  |
| REQ\_OPE\_3\_010 | Data quality. | Used AI algorithms or monitoring functions should implement a semantic-oriented policy to describe fine-grained details of data features (e.g., data range provided by a specific sensor, security levels) |  |  |
| 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 [2]). |  |  |
| REQ\_OPE\_4\_011 | Preservation of integrity, privacy and security | The data flow for safety applications shall be secured (see also [2]). |  |  |
| REQ\_OPE\_5\_001 | Data access. | Users shall possess the required authorization for accessing data. |  |  |

### -----------------------End of change 1-------------------------------------------