ETSI TR 103 778 V1.1.1 (2021-12)

TECHNICAL REPORT

SmartM2M;
Use cases for cross-domain data usability of IoT devices

Reference

DTR/SmartM2M-103778

Keywords

artificial intelligence, data usability, IoT, oneM2M,
use case

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

In June 2018 the EU Council endorsed an ambitious Europe-wide Coordinated AI Action Plan [i.7], where standardization plays a role to support interoperability and exchange of data and metadata across systems as crucial input of information to AI platforms, allowing them to be better filter information from "data lakes" and to create derivative information or decisions and integrity of data shared.

With the current pandemic, Government decisions have been seen to depend on the quality of information available at the present, which is based on the data gathered, its modelling and how the systems work and interact. This is increasingly being impacted by Artificial Intelligence. There are however risks identified for AI applications, for example concerning the acceleration of possibly inappropriate responses, concerning incorrect modelling or insufficient training data, concerning aspects of AI trust and explainability, and appropriate testing [i.8].

Standardization can help to reduce such risks, for example by establishing standards for comparative benchmarking, for certifying models, for validating model integrity, etc.

Current AI technologies based mainly on Machine Learning and on processing large amounts of data has led to a debate on data gathering, data ownership, data transparency, data bias that is going well beyond technical matters (privacy, regulation, remuneration schemes). The (negative) impact of poor-quality training data is very obvious, especially in health applications, road travel, etc. Due to the growing use of AI models in standards, ETSI Technical Bodies have decided to investigate means to assess the "quality" and usability of datasets needed to train and also to test the AI capabilities referenced by new standards [i.8] which is one of the motivations for this work.

IoT devices and platforms also provide data that are used directly by human and very often non-technical users. This is the case for example for medical teams and their patients in the medical sector, mechanics in the automotive sector or first responders in the emergency sector. Trust in the IoT system can be ensured only if these data bring in a real added-value and are delivered in a non-ambiguous manner to these users. To analyze how this can be ensured is another motivation for this work.

1 Scope

The objective of the present document is to identify, select and describe use cases where the IoT data and services require data usability specifications for machines consuming data for AI (for example machine learning). Enabling data usability with AI approach will also be considered.

The present document will document a formal description of the use cases and analyse the impact of these use cases from the data usability point of view.

It is very important to clarify that user experience (ergonomics) or the accessibility of the ICT equipment are out of scope of the present TR. The objective of the present document is only focused on the data generated and processed by IoT devices and platforms and consumed by human or machine (AI/ML) users. The present document is also:

- to identify, select and describe use cases where the IoT data and services require data usability specifications;
- to analyse the impact of these use cases for both machines and humans.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, Alliance for Internet of Things Innovation (AIOTI), January 2020.

[i.2] ISO 9241: "Ergonomics of human-system interaction" (multi-part standard).

[i.3] Lexico Dictionary.

NOTE: Available at https://www.lexico.com/definition/usability.

[i.4] Guidelines for the use of IoT related Standards in Smart Farming and Food Security (D3.5).

NOTE: Available at https://www.iof2020.eu/deliverables/d3.5-guidelines-for-the-use-of-iot-related-standards-in-smart-farming-and-food-security.pdf.

[i.5] oneM2M TR-0001 (V4.4.0): "oneM2M; Use Cases selection".

[i.6] ETSI GR ENI 001: "Experiential Networked Intelligence (ENI); ENI use cases".

[i.7] EC White Paper On Artificial Intelligence: "A European approach to excellence and trust", February 2020.

NOTE: Available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[i.8] ETSI White Paper: "Artificial Intelligence and future directions for ETSI".

[i.9] Directive 2011/24/EU of The European Parliament and of the council Of 9 March 2011 on the application of patients" rights in cross-border healthcare.

NOTE: Available at https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF.

[i.10] oneM2M TR 0026-(V4.5.0): "oneM2M; Vehicular Domain Enablement".

[i.11] ETSI TR 103 376: "SmartM2M; IoT LSP use cases and standards gaps".

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.13] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.14] VICINITY-D5-2-VICINITY-value-added services implementation framework-1.0.

NOTE: Available at VICINITY_D5.2_VICINITY_Value-added_services__implementation_framework_v1.0 (vicinity-h2020.eu).

[i.15] 3GPP TR 22.804: "Technical Specification Group Services and System Aspects; Study on Communication for Automation in Vertical Domains".

[i.16] MONICA Project.

NOTE: Available at https://www.monica-project.eu/applications.

[i.17] ETSI TR 103 582: "EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations".

[i.18] ETSI TR 103 509: "SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well".

[i.19] ETSI TR 103 510: "SmartM2M; SAREF extension investigation; Requirements for Wearables".

[i.20] ETSI GR SAI 004: "Securing Artificial Intelligence (SAI); Problem Statement".

[i.21] ETSI TR 103 546: "SmartM2M; Requirements & Feasibility study for Smart Lifts in IoT".

[i.22] ASSIST-IoT deliverable (D3.2): "Use Cases Manual & Requirements and Business Analysis".

[i.23] ETSI TR 103 477: "eHEALTH; Standardization use cases for eHealth".

[i.24] "Guidebook Component D; Data Usability and Analysis; Transportation Performance Management", Federal Highway Administration, US Department of Transportation.

NOTE: Available at TPM Guidebook Chapter 10 Summary | TPM Toolbox (tpmtools.org).

[i.25] ETSI TS 103 779: "SmartM2M; Requirements and Guidelines for cross-domain data usability of IoT devices".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

artificial intelligence: ability of a system to handle representations, both explicit and implicit, and procedures to perform tasks that would be considered intelligent if performed by a human [i.20]

data usability: ability of a user to derive useful information from data [i.24]

usability: degree to which something is able or fit to be used [i.3]

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABS	Anti-lock Braking System
AD	Autonomous Driving
ADApp	Autonomous Driving application
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/Machine Learning
AR	Augmented Reality
AS	Application Servers
BIM	Building Information Modelling
CCTV	Closed-Circuit Television
CHE	Container Handling Equipment
CPU	Computing Processing Unit
DC	Data Center
DDOS	Distributed Denial Of Service
DevOp	Development and Operation
DSS	Decision Support System
DVR	Dashboard Video Recorder
EC	Emergency Call
EGW	Energy GateWay
EHR	Electronic Health Records
ENI	Experiential Networked Intelligence
GB	Giga Byte
GPS	Global Positioning System
H/M/L	High/Medium/Low
HEM	Home Energy Management
I/O	Input and Output
ICT	Information and Communication Technologies
ID	IDentifier
IoT	Internet of Things
ISE	In-Service Emissions
IT	Information Technology
LDM	Local Dynamic Map
LIDAR	LIght Detection And Ranging
M2M	Machine to Machine
MANO	Management and Orchestration
ML	Machine Learning
MONICA	MONitoring trends and determinants In CArdiovascular disease
N/A	Not applicable
NFV	Network Function Virtualisation
NG-IoT	Next Generation IoT
OCR	Optical Character Recognition
OS	Operating Systems
OSH	Occupational Safety and Health
OSS	Operations Support System
PC	Personal Computer
PDS	Position Detection System
PHR	Personal Health Records
PPE	Personal Protective Equipment
PPM	Privacy Policy Manager
PSAP	Public-Safety Answering Point
RAM	Random Access Memory
RMG	Rail Mounted Gantry cranes
RTG	Rubber Tired Gantry cranes

SLA	Service Level Agreement
SP	Service Provider
STF	Specialist Task Force
STS	Ship-To-Shore cranes
TOS	Terminal Operating System
TT	Terminal Tractor
TV	TeleVision
UC	Use Case
UC-P2	Use Case -Position 2
UV	UltraViolet
VIP	Very Important Person
VM	Virtual Machines
VNF	Virtualised Network Functions
WCDMA	Wideband Code Division Multiple Access

4 Background

4.1 Motivation

Data usability of services that the IoT devices and platforms deliver is a key issue not yet addressed. In fact, a few standards on data usability exist but they are only based on the user experience (ergonomics) or the accessibility of the ICT equipment. For addressing the Data usability of the data and services that the IoT devices and platforms deliver an effective Knowledge Representation should be employed to enable it at the two fundamental levels: the first one for the organization of the information itself, the second level for the information presentation. To be able to achieve those IoT data usability objectives, Artificial Intelligence (AI) employment is required.

Usability and more specifically data usability have been identified as a gap in the results of ETSI TR 103 376 [i.11] (tools to enable ease of installation, configuration and personalization; usability and convenience in Table 58, usability and customization of the solutions: to address different market sub-segments and simplify their usage by the large public in clause 9.4 of [i.11]). The outcome of the standardization gap analysis performed by AIOTI in 2019 [i.1] has shown that this gap is not yet covered (see section 6.8 of the report).

Standards on usability exist, however they are based on "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [i.2], in practice the user experience (ergonomics) or the accessibility of the ICT equipment. Due to the massive introduction of IoT devices, the data usability topic should also be considered from a data and service point of view.

IoT technologies are one of the technologies which are contributing to the digital transformation of many verticals, together with big data and AI. Standardizing the usability of data and services from IoT devices and platforms would have a strong impact on these two technologies. Indeed, data usability can be considered as a consumer and an enabler of AI, as follows:

- 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 increases the reliability of the data used by AI.

Note that knowledge representation is reflected in ontologies, limited or extended by their domain specific availability.

The objective of this work is to cover a missing key link of the IoT eco-system chain.

The work should identify use cases where the IoT data and services require data usability specifications. The data that IoT devices and platforms provide should be easily accessed, understood and acted upon by a large non-technical public in the case of humans (e.g. medical teams and their patients in the medical sector, mechanics in the automotive sector, first responders in the emergency sector, etc.) and by machines and processes when the data are fed to the AI components of a system (e.g. machine learning).

This also means that the IoT technologies, devices and platforms themselves can be trustily used according to their initial objectives (e.g. easy installation, configuration, operation and maintenance).

Based on these use cases, requirements and guidelines will be derived towards a horizontal cross-domain standard, with the specification of minimum requirements for data usability of professional and general public IoT services, whether they are critical or not. The diagram below shows the link between the present document and the specification document.

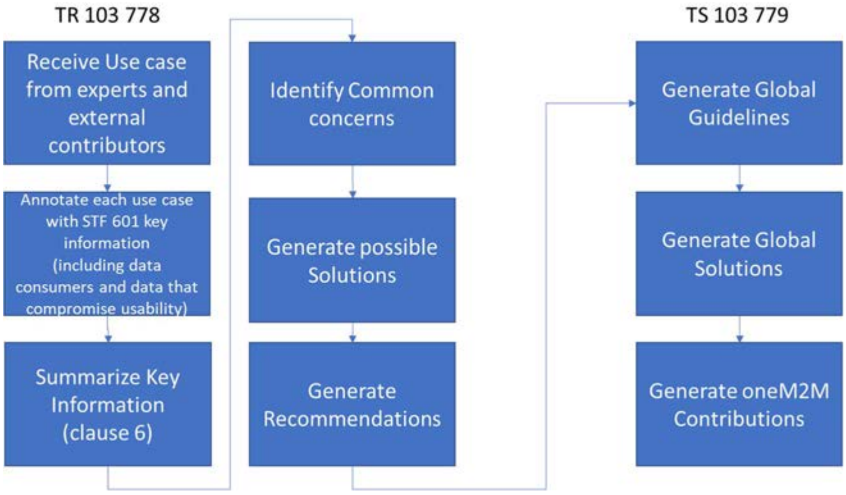
TR 103 778
Receive Use case from experts and external contributors
Annotate each use case with STF 601 key information (including data consumers and data that compromise usability)
Summarize Key Information (clause 6)
Identify Common concerns
Generate possible Solutions
Generate Recommendations
TS 103 779
Generate Global Guidelines
Generate Global Solutions
Generate oneM2M Contributions

Figure 4.1-1: Link between the use cases and the specifications

4.2 Human intervention in AI systems

Human oversight helps ensuring that an AI system does not undermine human autonomy or cause other adverse effects [i.7]. The objective of trustworthy, ethical and human-centric AI can only be achieved by ensuring an appropriate involvement by human beings in relation to high-risk AI applications.

It will also be without prejudice to the legal rights established by the GDPR when the AI system processes personal data. For instance, human oversight could have the following, non-exhaustive, manifestations:

- the output of the AI system does not become effective unless it has been previously reviewed and validated by a human (e.g. the rejection of an application for social security benefits may be taken by a human only);
- the output of the AI system becomes immediately effective, but human intervention is ensured afterwards (e.g. the rejection of an application for a credit card may be processed by an AI system, but human review should be possible afterwards);
- monitoring of the AI system while in operation and the ability to intervene in real time and deactivate (e.g. a stop button or procedure is available in a driverless car when a human determines that car operation is not safe);
- in the design phase, by imposing operational constraints on the AI system (e.g. a driverless car will stop operating in certain conditions of low visibility when sensors may become less reliable or will maintain a certain distance in any given condition from the preceding vehicle).

4.3 Clarifying the notion of data usability of IoT devices

Data usability from the human data consumer point of view means that the information and data generated by an IoT platform and provided to a human user is in a form ready for, or easily prepared, for consumption by this user, without any possible ambiguity on its meaning. Consumption by human users most likely means usable for natural language-like queries (not cryptic) and answers, without the need for complex processing. It also allows the user to apprehend the volume and repetition of the IoT data. For example, the result may be integrated with a home assistant or smart speaker.

Data usability from the machine data consumer point of view means that the information and data generated by an IoT platform is presented in a form ready for, or easily prepared, for consumption by a machine learning algorithm, or any other type of Artificial Intelligence (AI) algorithm, without the possibility to misinterpret the data, for example by inverting the values obtained by two different sensors.

Data usability by machines and human data consumers implies transparency and trust (understand how it works), safety and acceptability of the data provided by an IoT platform. Together with data integrity, data consistency, etc. it is an essential component of data quality.

Lack of data usability means that the information and data generated by an IoT platform may be used improperly or misinterpreted.

4.4 Objective of the use case analysis

The use cases presented in clause 5 are collected from real life scenarios, industries, and practices. What the present document presents is the analysis of these use cases from the "use of data generated" viewpoint.

The domain areas covered by the use cases in clause 5 are as follows:

- Health Care
- Public and Emergency Services
- Industry and Manufacturing
- ICT Network Management
- Agriculture and Farming
- Energy
- Building
- Retail
- Large Events
- Smart Lifts
- Smart Cities

Many of the use cases may also trigger concerns about the privacy of the IoT data and the cyber-security of the related devices and processes. These topics are addressed in detail in ETSI TR 103 533 [i.12] and ETSI TR 103 591 [i.13]. The present document considers that both issues, when relevant to the use cases of clause 5, have been addressed separately and resolved.

5 Use Cases

5.1 Health Care Use Case

5.1.1 Use Case A.1: Adoption of an AI-based system for supporting patients

5.1.1.1 Description

Diets and physical activity play a crucial role for a long and healthy life. Indeed, monitoring eating habits of users will help to prevent different types of pathologies, chronic diseases and cognitive decline. However, engaging people in developing and maintaining healthier patterns of living is a challenging task. For example, redirecting a user from eating unhealthy foods requires suggesting viable alternatives. Those alternatives can be based on rational food properties or more abstract concepts such as taste. This would be done through an interface for personal devices able to collect data from the user, wearable sensors, and contextual data. Furthermore, to provide real-time feedback and notify the user with persuasive and motivational messages, adapted representation, such as text, speech, video, or graphical alerts, are also required.

Diet oriented concepts and ontologies concerning the food domain are necessary in order to specify all the relevant information such as the number of calories and nutrients consumed in a given meal. Therefore, the detailed description about each food and food properties should be established. Furthermore, an intelligent platform allowing experts to propose monitoring rules and guidelines regarding a healthy lifestyle that users should adapt for maintaining their physical and mental wellbeing would be used. External events would occur as a trigger for the system, for instance a user eating too much food or performing too low in physical activity.

Equipped with body sensor networks, wearable sensors and mobile smart devices for health monitoring, the goal is the development of an eHealth system through the integration of several IoT platforms and medical sensors. Via the monitoring of user's lifestyle in a decentralized and mobile manner, health issues caused by inappropriate diet and lack of physical activity would be prevented. These monitoring processes are meant to be decentralized from the healthcare centre to the monitored subjects' homes, as well as supported in mobility situations by using on-body physical activity monitors.

The strategic importance of such complete use case is largely motivated by the fact that unhealthy, such as improper and hyper-calorie diet and insufficient physical activity, are the base of main chronic diseases.

5.1.1.2 Source

- ETSI TR 103 509 [i.18].
- ETSI TR 103 510 [i.19].

5.1.1.3 Actors

- ***[Human]:*** Physicians: which can monitor the health status of their patients and to check if there are some behaviours that are not compliant with respect to their guidelines (e.g. patients that have to avoid some specific foods or activities) and/or if there are some dangerous situations (e.g. undesired episodes of people affected by asthma). Moreover, physicians can define sets of user-specific monitoring rules and to assign them to their patients.
- ***[Human]:*** Patients, which can receive a notice if they do not respect assigned guidelines or if some warning situations have been detected. Patients, are defined as people affected by one or more disease/s.
- ***[Human]:*** Users, which can receive a notice if they do not respect assigned guidelines. Users, are defined as people that are not affected by any disease.
- ***[Machine]:*** AI engine, which is in charge of acquiring data explicitly provided by users and/or acquired through sensors. The AI engine applies a strategy (e.g. statistical, symbolic, or mixed) for verifying the compliance of acquired data with respect to the guidelines and monitoring rules defined by physicians.
- **Data user/consumer:** Physicians, Patients, Users, AI engine.

5.1.1.4 Pre-conditions

- The physicians' monitoring platform, the patients' and users' smartphone applications, and the IoT devices are deployed and in operational condition.
- The AI engine services are up and running.

5.1.1.5 Triggers

- The AI engine detects a set of data that is not compliant with respect to the guidelines that a given physician assigned to a specific user.
- The AI engine detects a set of data highlighting a potentially dangerous situation in a patient affected by a specific disease.

5.1.1.6 Normal Flow

- The user (or the patient) provides data about consumed food and performed activity through the use of mobile application and/or devices like smartwatches.

- The system stores the data into a knowledge graph and performs reasoning activities for detecting potential undesired behaviours by matching user's (or the patient's) data with the guidelines provided in advance by the physician.
- If an undesired behaviour is detected, the user (or the patient) is alerted about the undesired event together with the related explanation.
- Together with the user (or the patient), the physician is alerted as well in order to make her aware about the violated guideline.
- The system keeps track of the event and updates the policies used for generating the next feedback in the case that the same undesired event would be detected.

5.1.1.7 Alternative Flow

None.

5.1.1.8 Post-conditions

The physician and the patient (or the user) are informed about the dangerous (or undesired) situation through the notification manager integrated within the AI engine.

5.1.1.9 High Level Illustration

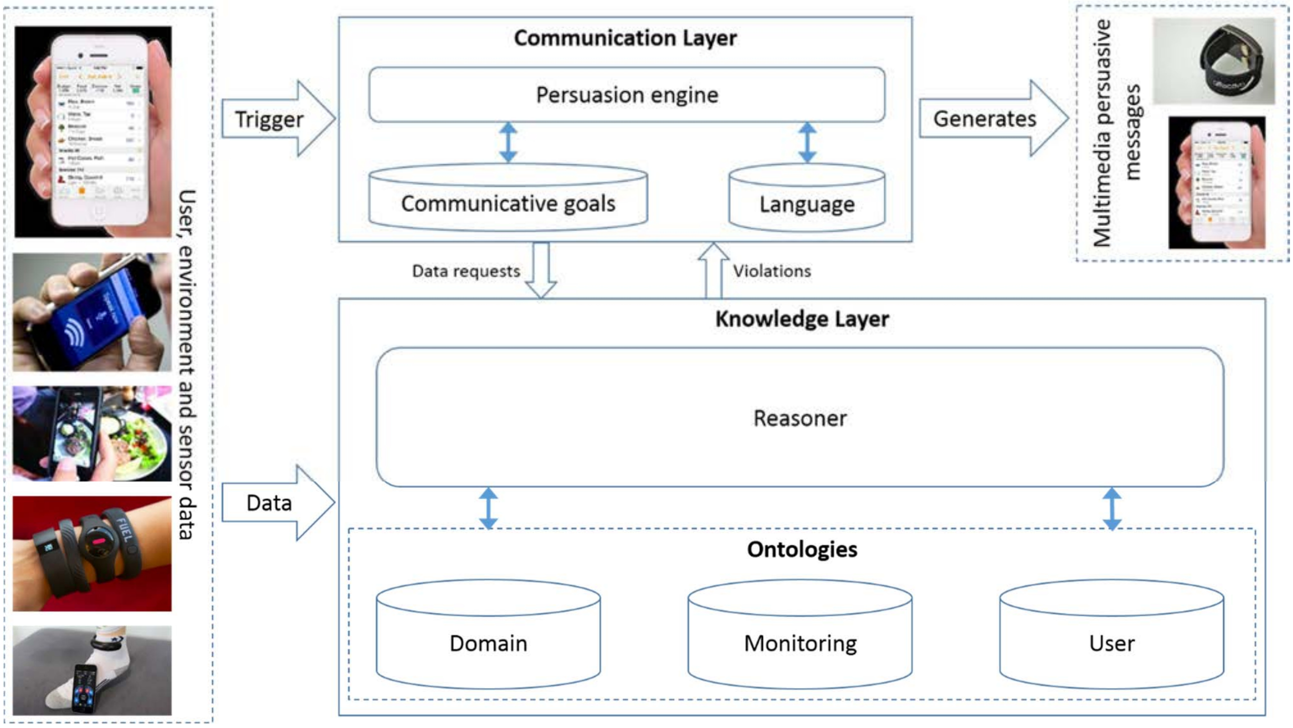

Figure 5.1.1.9-1: High level illustration of the described use case

5.1.1.10 Use case analysis

Clause 5.1.1.1 provides an extensive description of the use case.

Here, the focus is on the risks connected with the amount of data provided by both patients (or users) and IoT devices to the AI engine.

Data that may compromise data usability:

- Data provided explicitly by users.

- Data provided by IoT devices.

Indeed, the adoption of IoT technology can create new safety risks if it is not designed appropriately, implemented carefully, and used thoughtfully. Data integrity errors as a result of incorrect or missing data in the patient's Electronic Health Records (EHRs) and other health IT systems are a crucial issue in the healthcare sector that can dramatically affect patients (and users) health. Data integrity issues occurred with the use of paper medical records as well, but now, as EHRs become more interoperable and hackable, incorrect information is more readily available, more easily shared, and harder to eliminate. One patient's data appearing in another patient's record, missing data or delayed data delivery, and clock synchronization errors between medical devices and systems are examples of data integrity failures.

These issues can lead to wrong inference or classification outcomes by the AI engine with the consequence of providing wrong information to the physicians and, even worse, compromising patients' health

5.1.2 Use Case A.2: Electronic Health records

5.1.2.1 Description

Diagnostic and preventative medicine requires access to a valid and accurate record of patient health over as long a period as possible. Thus, whilst it may be argued that health devices (heart rate monitors, blood pressure monitors and so forth) are critical, they are only critical if the readings they take are recorded, and as is suggested in the use case statement, identify with some accuracy the context of the reading. Health records are required to cross international borders as has been explicitly stated in Directive 2011/24/EU [i.9] on patients' rights in cross-border healthcare.

A health record is a composite document and one of the difficulties surrounding the definition of a health record is in establishment of the boundary. In the domain of diagnostic medicine information is required to establish context. For example, many illnesses in their early stages have shared symptoms and to accurately attribute symptom to cause may mean the difference between survival and not.

A health record has no fixed start time and end time. Whilst for an individual a health record exists from birth, there are aspects of the individual's health that are directly linked to the parents (e.g. genetics) and to the period in the womb that need to be linked to the individual's record. Associated to the individual's record are also records of the health professionals, of the locations at which medical interventions occur (e.g. hospital, clinic), and of the medications prescribed, and so on.

AI-based systems continuously run-in background by building a patient context from the content of personal electronic health records and by linking it with external knowledge in order to support clinicians in their work (e.g. early diagnosis).

5.1.2.2 Source

Derived from ETSI TR 103 477 [i.23].

5.1.2.3 Actors

- ***[Humans]:*** Physicians, which can monitor the health status of their patients and check if there are some patterns need attention of trigger further verifications.

- ***[Humans]:*** Patients, which can receive a notice about the need of performing specific verifications if the physician accepts the AI engine suggestion.

- ***[Organization]:*** Healthcare Organizations, which can benefit of AI-based solutions by running prevention campaigns that in the middle/long-term can both reduce the healthcare costs and improve the overall population health.

- ***[Machine]:*** AI engine, which is in charge of acquiring data explicitly provided by users, acquired through sensors, or inputted by physicians. The AI engine can apply strategies (e.g. statistical, symbolic, or mixed) for running predictive analysis operations with the aim of, for example, early detecting the possible onset of diseases.

- **Data user/consumer:** Physicians, Patients, Healthcare Organizations, AI engine.

5.1.2.4 Pre-conditions

- The data management system in charge of collecting all data is operational.
- Physicians are equipped with a working tool enabling the input of patient data into the data management system.
- Patients can be equipped with a mobile application and/or IoT devices for collecting information that are saved into their personal health records.
- IoT devices are working and connected to the network.
- AI-based service is working.

5.1.2.5 Triggers

New data are provided into an electronic health record.

5.1.2.6 Normal flow

- New information is stored into the electronic health record of a given patient by the physician.
- The AI engine updates the digital twin of the patient with the new information and run a check process for discovering possible scenarios leading to the onset of a diseases.
- The AI engine suggests to the physician that further verifications should be performed.
- The physician observed that the sugar blood is close to the attention level and prescribe a diet to the patient for avoiding nutritional exacerbations.

5.1.2.7 Alternative flow

None.

5.1.2.8 Post-conditions

The patient entered into a monitored pathway that, starting early, avoids the onset of nutritional diseases.

5.1.2.9 High Level Illustration

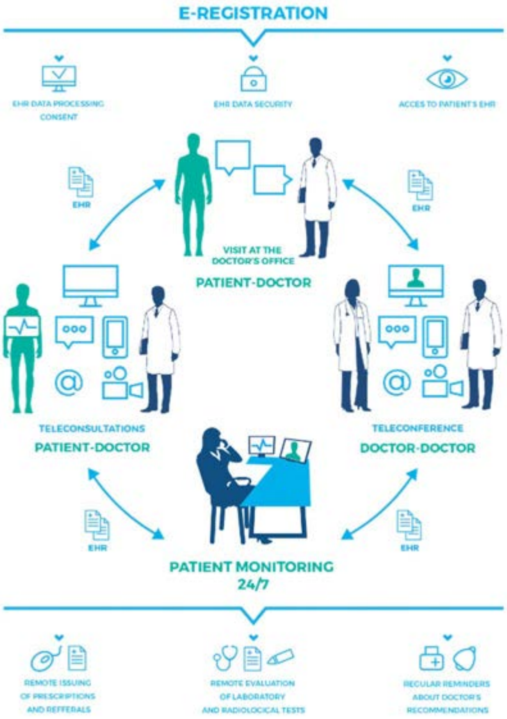
E-REGISTRATION
EHR DATA PROCESSING CONSENT
EHR DATA SECURITY
ACCES TO PATIENT'S EHR
EHR
EHR
VISIT AT THE DOCTOR'S OFFICE
PATIENT-DOCTOR
TELECONSULTATIONS
PATIENT-DOCTOR
TELECONFERENCE
DOCTOR-DOCTOR
EHR
EHR
PATIENT MONITORING 24/7
REMOTE ISSUING OF PRESCRIPTIONS AND REFFERALS
REMOTE EVALUATION OF LABORATORY AND RADIOLOGICAL TESTS
REGULAR REMINDERS ABOUT DOCTOR'S RECOMMENDATIONS

Figure 5.1.2.9-1: Electronic health record

5.1.2.10 Use case analysis

Data that may compromise data usability:

- Information provided by clinicians.
- Device and IoT data (when used).

Information provided by clinicians are not properly stored into the system due to issues related to the format of such information or to some failures of the network. If IoT data are exploited, potential issues are linked to IoT devices that do not provide data according with the fine-grained level required or are not provided at all due to some failures. Moreover, the sensors can be affected by false reading issues than can affect the overall data usability of the patient's PHR.

5.1.3 Use Case A.3: Diagnostic eHealth

5.1.3.1 Description

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. For many aspects, this use case is similar to the one described within the use case A.2 since the type of managed information are the same. What is different is the purpose for which such information are used. Within the previous use case provided information are used exclusively for building the digital twin of patients. In this use case, information provided are combined with the ones available from the digital twin, merged with medical knowledge and exploited for suggesting a possible diagnosis associated with an undesired event occurred to a patient.

As identified in [i.23] data transfer requirements may be identified in an abstract form using a set of attributes that the date transfer scheme has to meet. Such attributes together with their descriptions are presented in [i.1], clause 6.2.

5.1.3.2 Source

Derived from ETSI TR 103 477 [i.23].

5.1.3.3 Actors

- ***[Humans]:*** Physicians, which can monitor the health status of their patients and check if there are some patterns need attention of trigger further verifications.
- ***[Humans]:*** Patients, which can receive a notice about the need of performing specific verifications if the physician accepts the AI engine suggestion.
- ***[Organization]:*** Healthcare Organizations, which can benefit of AI-based solutions by running prevention campaigns that in the middle/long-term can both reduce the healthcare costs and improve the overall population health.
- ***[Machine]:*** AI engine, which is in charge of acquiring data explicitly provided by users, acquired through sensors, or inputted by physicians. The AI engine can apply strategies (e.g. statistical, symbolic, or mixed) for running predictive analysis operations with the aim of, for example, early detecting the possible onset of diseases.
- **Data user/consumer:** Physicians, Patients, Healthcare Organizations, AI engine.

5.1.3.4 Pre-conditions

- The data management system in charge of collecting all data is operational.
- Physicians are equipped with a working tool enabling the input of patient data into the data management system.
- IoT devices are working and connected to the network.
- AI-based service is working.

5.1.3.5 Triggers

New data are provided into an electronic health record.

5.1.3.6 Normal flow

- New information is stored into the electronic health record of a given patient by the physician.
- The AI engine updates the digital twin of the patient with the new information and run a check process for discovering possible scenarios leading to the onset of a diseases.
- The AI engine suggests to the physician that further verifications should be performed.
- The physician observed that the sugar blood is close to the attention level and prescribe a diet to the patient for avoiding nutritional exacerbations.

5.1.3.7 Alternative flow

None.

5.1.3.8 Post-conditions

The patient entered into a monitored pathway that, starting early, avoids the onset of nutritional diseases.

5.1.3.9 High Level Illustration

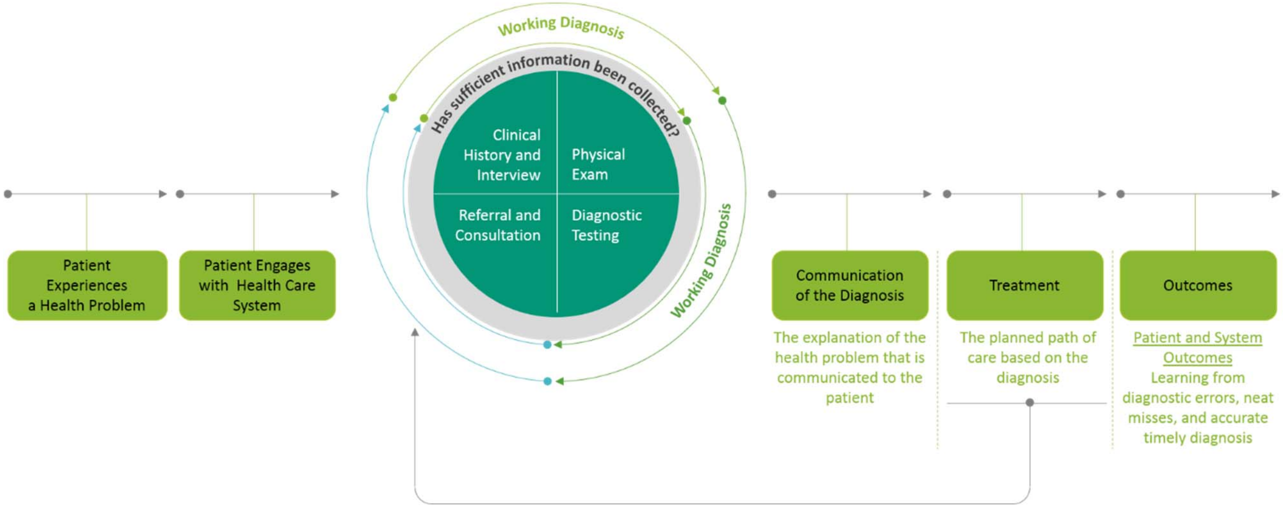
Working Diagnosis
Has sufficient information been collected?
Clinical History and Interview
Physical Exam
Referral and Consultation
Diagnostic Testing
Working Diagnosis
Patient Experiences a Health Problem
Patient Engages with Health Care System
Communication of the Diagnosis
Treatment
Outcomes
The explanation of the health problem that is communicated to the patient
The planned path of care based on the diagnosis
Patient and System Outcomes
Learning from diagnostic errors, neat misses, and accurate timely diagnosis

Figure 5.1.3.9-1: Diagnostic eHealth

5.1.3.10 Use case analysis

Data that may compromise data usability:

- 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.

Considering an example of the use of devices like smart spirometers for assessing the pulmonary function of patients affected by asthma. During measurement operations, if the values read by the IoT sensor is not precise, the pulmonologist will work with on a patient's digital twin containing wrong information. This way, the decision support system adopted by the pulmonologist will be compromised and the provided diagnosis not correct with respect to the actual patient's condition.

5.1.4 Use Case A.4: Clinical intervention

5.1.4.1 Description

This case addresses the challenge of monitoring the stimulus that a medical actuator delivers at a certain time to a specific patient in a given context.

In general, clinical intervention should follow a prescribed diagnostic and treatment strategy. Thus, it is suggested that delivery of drugs or other clinical/medical treatment should be traceable to specific recommendations from the diagnostic analysis. Hence, this use case, as well, can be considered a follow up of the use cases described in use cases A.2 and A.3.

The following are forms of clinical intervention that may be augmented by eHealth technologies.

Firsts are non-surgical intervention, like drug monitoring and dose control or physical well-being control. In this use case the context refers to the set of diagnostic measurements that indicate that a stimulus is required, e.g. the measure of blood-sugar in the blood indicating a requirement for an injection of insulin to the blood.

Seconds are surgical intervention, like ICT assisted/enabled surgery or mechanical and ICT performed surgery.

In the first case, sensors and actuators required to perform surgery have to operate in real-time (or as close to as is practical), but decisions are made by a human operator. This conforms closely to the state of play today in which surgical procedures are made safe using eHealth technologies. This scenario can be extended by considering those parts of surgical intervention that may only be enabled by eHealth equipment. This conforms to many of the advanced keyhole and micro-surgeries that are enabled by eHealth technologies where unassisted and unenabled surgery would be impossible. Instead, in the second case, surgeries are performed without direct human involvement.

5.1.4.2 Source

Derived from ETSI TR 103 477 [i.23].

5.1.4.3 Actors

- ***[Humans]:*** Physicians, which can monitor the health status of their patients and check if there are some patterns need attention of trigger further verifications.
- ***[Humans]:*** Patients, which can receive a notice about the need of performing specific verifications if the physician accepts the AI engine suggestion.
- ***[Organization]:*** Healthcare Organizations, which can benefit of AI-based solutions by running prevention campaigns that in the middle/long-term can both reduce the healthcare costs and improve the overall population health.
- ***[Machine]:*** AI engine, which is in charge of acquiring data explicitly provided by users, acquired through sensors, or inputted by physicians. The AI engine can apply strategies (e.g. statistical, symbolic, or mixed) for running predictive analysis operations with the aim of, for example, early detecting the possible onset of diseases.
- **Data user/consumer:** Physicians, Patients, Healthcare Organizations, AI engine.

5.1.4.4 Pre-conditions

- The data management system in charge of collecting all data is operational.
- Physicians are equipped with a working tool enabling the input of patient data into the data management system.
- Patients can be equipped with a mobile application and/or IoT devices for collecting information that are saved into their personal health records.
- IoT devices are working and connected to the network.
- AI-based service is working.

5.1.4.5 Triggers

New data are provided into an electronic health record.

5.1.4.6 Normal flow

- New information is acquired from an ecosystem of diagnostic sensors.
- The physician input her observations too in order to enable the AI engine to merge them.
- The AI engine updates the digital twin of the patient with the information acquired and generate a recommendation about the most effective treatment to deliver.
- The physician decides if the treatment should be adjusted or not and delivers it to the patient.

5.1.4.7 Alternative flow

None.

5.1.4.8 Post-conditions

The patient benefits from a personalized treatment.

5.1.4.9 High Level Illustration

Figure 5.1.4.9-1: Clinical intervention

5.1.4.10 Use case analysis

Data that may compromise data usability:

- Information provided by patients (first case).
- Information provided by clinicians (first and second case).
- Device and IoT data (when used) (first and second case).

As mentioned in clause 5.1.4.1, there are two possible scenarios that can be addressed within this use case. In the first one, the intervention is related to new behaviours that patients have to follow. Here, information provided by patients are crucial for keeping the AI system usable and effective.

As example, if the patient provides coarse-grained information, the AI system might work with ambiguous information that might compromise the intelligent component of the system. The result will be a wrong monitoring operation with the consequence of providing wrong feedback.

Instead, within the second scenario the AI is more invasive since the intervention includes surgeries. Here, the fine-grained level and the correctness of the data provided by sensors and actuators are crucial for avoiding dangerous issues. Together with the data provided by both sensors and actuators, also information provided by clinicians are critical as well since they are used for setting up the clinical intervention.

5.2 Public and Emergency Services Use Cases

5.2.1 Use Case B.1: Automatic direct emergency call from IoT device

5.2.1.1 Description

This use case applies to an emergency event when a smoke or temperature detector in a remote location (forest, remote facility, etc.) sends an emergency message in the event of a fire.

The IoT device initiates the emergency call (probably to a local aggregating platform) which triggers an alert at the platform operator responsible to call public safety. However, when the operator tries to confirm that a fire has started, he fails and estimates that it was a false alert. Thirty minutes later, a second sensor raises another identical alert. This time, the operator can validate the alert, however the fire has now grown to enormous size, it is more difficult to be extinguished and the remote facility is almost entirely destroyed.

NOTE: This use case applies to a large building or a remote location. A person calling emergency services with a smartphone from home does not directly apply to this use case.

5.2.1.2 Source

Derived from ETSI TR 103 582 [i.17], Automatic direct emergency call from IoT device.

5.2.1.3 Actors

- ***[Device]:*** IoT sensors, of different type (water, temperature, smoke) located in a remote and difficult to access location. Several sensors are distributed in the geographical area to enable redundancy of the alert. This use case is less relevant in case of locations where people can call directly using their smartphones.
- ***[Machine]:*** IoT platform monitoring the status of the sensors and providing a control console.
- ***[Human]:*** IoT platform operator and decision maker.
- **Data user/consumer:** The operator who handles IoT data received from the sensors. This operator may be human or an automatic process (AI).

5.2.1.4 Pre-conditions

- The IoT devices and IoT service platforms are deployed and in operational condition.
- The emergency services are established and functional.

5.2.1.5 Triggers

One of the IoT sensors detects parameters levels that constitute an emergency event according to its normal configuration.

5.2.1.6 Normal flow

This first flow describes the successful completion of the event in the case of a human user (nominal operation):

1) The IoT sensor detects an emergency event. It creates an emergency data message and forwards it to the IoT platform.

2) The platform receives the emergency data call, recognizes it as emergency data and raises an alert to the operator.

3) The operator retrieves and analyses the message and contacts the appropriate public safety services, sharing the contents of said messages.

4) Emergency services arrive early and are able to control the fire.

In the case described here, the completion is unsuccessful:

1) The IoT sensor detects an emergency event. It creates an emergency data message and forwards it to the IoT platform.

2) The platform receives the emergency data call, recognizes it as emergency data and raises an alert to the operator.

3) The operator retrieves and analyses the message. The operator requests local visual verification (camera or human), but is not able to validate the event.

4) The operator decides that this was yet another false alarm, as several took place in the previous days. The event is dropped.

5) Thirty minutes later, another sensor located in a close area raises the same event.

6) The operator retrieves and analyses the new message. The operator requests local visual verification (camera or human), and this time, is able to validate the event.

7) The operator contacts the appropriate public safety services, sharing the contents of said messages.

8) The fire has now grown to enormous size; it is more difficult to be extinguished and the remote facility is almost entirely destroyed.

5.2.1.7 Alternative flow

Similar flow, this time involving AI for the validation step.

5.2.1.8 Post-conditions

The emergency has been dealt with by the appropriate authorities aided by data from the IoT sensors. The IoT sensors are reset, tested for correct operation, and resume monitoring.

In the unsuccessful completion, an inquiry is started that determines that the first sensor provided an incorrect localization, preventing the successful confirmation by the operator of the initial alert.

Furthermore, a lack of maintenance of the IoT platform led to a large number of false alarms, reducing the level of trust of the operator.

5.2.1.9 High Level Illustration

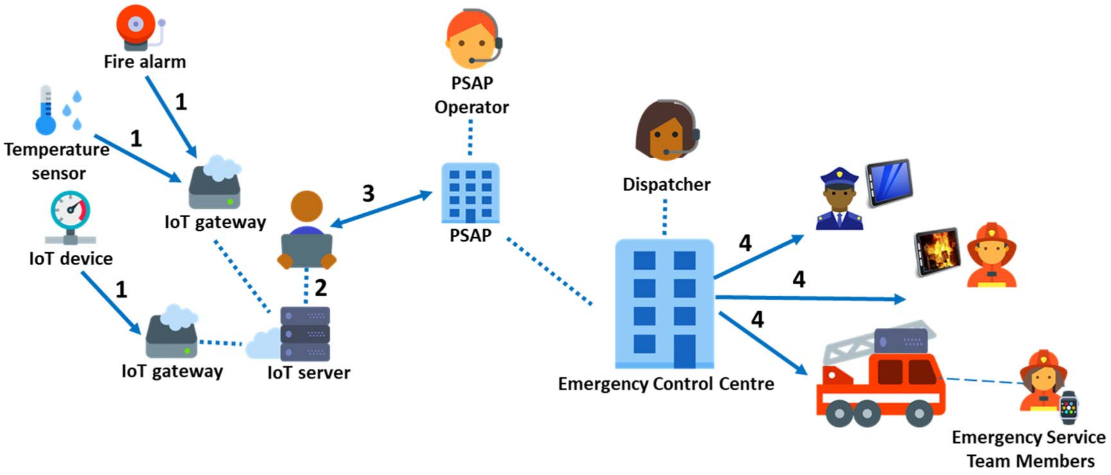

Figure 5.2.1.9-1: Illustration of automatic emergency call from IoT device

5.2.1.10 Use case analysis

Data that may compromise data usability:

- Geolocation of alarms.
- Sensor data.

In the case of the normal flow (nominal operation), data may be compromised if the system is not setup properly (location of the sensors is improperly configured) or the system maintenance is insufficient to ensure that the sensors are in working condition and do not trigger false positives.

In the case of the normal flow (unsuccessful completion), the operator has been provided with two series of non-usable data that led to a disaster:

- false alarms due to the lack of maintenance of the IoT platform and its sensors;

- wrong location information of the first sensor (probably due the wrong configuration of the system).

This is the same or even more important if the IoT platform is programmed to automatically validate the alarm.

The consequences of failing this use case because the data became unusable at some point in time may be very important: forest, remote facility, building completely destroyed with potentially loss of human/animal lives.

5.2.2 Use Case B.2: Emergency services teams accessing pre-deployed IoT devices

5.2.2.1 Description

This use case applies to an emergency event when emergency services, (e.g. firefighters) need to access data from IoT devices deployed in a smart building, for example smoke/heat detectors, surveillance cameras, but also devices in elevator cabins. These data could help them better focus their operation in case of fire for example, to locate people remaining on site, places where the fire is raging, etc.

Unless there are control rooms (with personnel operating the technology) emergency services normally do not have an immediate access to other IoT devices like surveillance cameras, etc., pre-deployed in a building. The IoT devices in this case belong to the building administration and management such that only the data they produce are shared on demand with the emergency services. Emergency services normally do not have access to these IoT devices.

5.2.2.2 Source

Derived from ETSI TR 103 582 [i.17], Emergency services teams accessing pre-deployed IoT devices.

5.2.2.3 Actors

- ***[Human]:*** Emergency service(s) decision maker(s) with a mandate to access a building's safety system;
- ***[Machine]:*** IoT service platform in the smart building;
- ***[Device]:*** Sensors/actuators pre-deployed in the building;
- **Data user/consumer:** The emergency services who will use the data from the building system to make their operation more efficient.

5.2.2.4 Pre-conditions

- An emergency event is occurring in a private or public building or in an area with pre-deployed IoT-based safety systems.
- There are IoT devices in the building's safety system that can provide additional helpful information to emergency service teams.

5.2.2.5 Triggers

The emergency service decision maker determines that he/she needs the additional information from the building's safety system.

5.2.2.6 Normal flow

This flow describes the successful completion of the event in the case of a human user (nominal operation):

1) An emergency service decision maker asks the authenticating entity for access to a building's safety system.

2) The authenticating entity grants access.

3) The emergency service decision maker can obtain IoT devices data via the IoT service platform from the building's safety system.

5.2.2.7 Alternative flow

None available here.

5.2.2.8 Post-conditions

Termination of the data connection between emergency service team and building safety system.

5.2.2.9 High Level Illustration

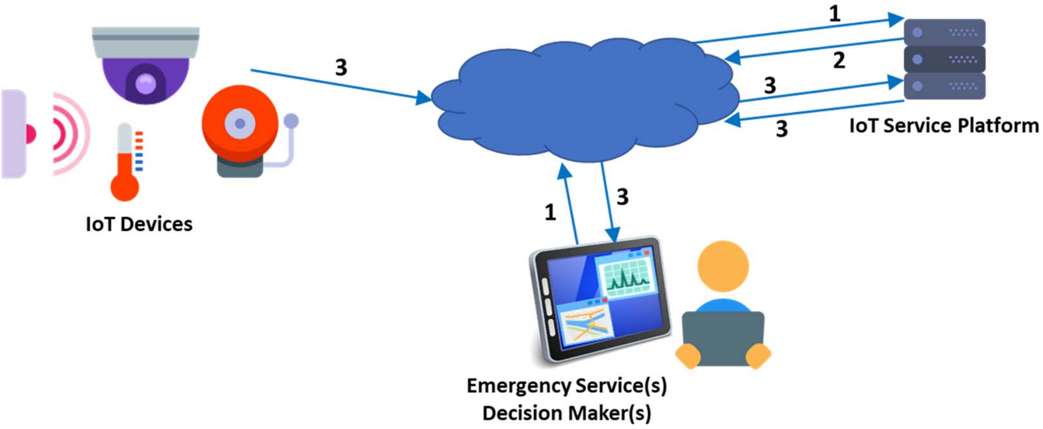

Figure 5.2.2.9-1: Illustration of an emergency service decision maker requesting access to pre-deployed IoT devices

5.2.2.10 Use case analysis

Data that may compromise data usability:

- Sensor data provided by the building IoT platform and their semantics.
- Security authentication data that may prevent the emergency services from accessing and using the building data.

In the flow described in clause 5.2.2.6, the completion may be unsuccessful if:

- The emergency service team's devices are not granted access by authenticating entity.
- The emergency service team's devices are not compatible to data provided by the building's safety system.
- The emergency service team's devices misinterpret the data provided by the building's safety system which hinders the efficiency of the whole rescue operation.

IoT data are usable in the case where their access is fully granted to people who may need to access them. Lack of interoperability at data level between systems (e.g. semantics unknown) may prevent usability of these data.

The consequences of failing this use case because the data are unusable as described above may be very important: building completely destroyed with potentially loss of human lives.

5.2.3 Use Case B.3: Cooperative Fog Services with Drones

5.2.3.1 Description

Drones with fog capabilities can be operated in many environments and applications, such as supply chain delivery, environment surveillance and video broadcasting, providing near real-time adjustments and collaboration in response to anomalies, operational changes or threats. With various capabilities such as computing, sensing, video recording, data storage, and communicating, drones can act as fog nodes, which interoperate and cooperate as a dynamic community to efficiently distribute services across compute, storage, networking, security, and other functions.

In many scenarios, a request of fog service may require a cluster of drones to operate cooperatively to provide the required capabilities and complete the task, since each drone itself is limited by the capabilities or coverage. In this case, the fog service request will first be split into smaller "pieces" with each piece containing a portion of capability requirements, such that they can be handled by the fog nodes jointly. For example, in an environment surveillance scenario, each drone can only monitor a limited area, so surveillance over a large area may require the combination and synergy from multiple drones' monitoring where each drone is responsible for a sub-area under its coverage. Similarly, a computation intensive video analysis task may exhaust the battery of a drone rapidly, or the limited computation speed of a drone cannot meet the real-time processing requirements, in which case the task can be split and distributed to multiple drones to be completed efficiently. Moreover, a drone may need another's communication capability to help relay messages to a destination out of its reach.

The cooperation is also necessary when considering the dynamic availability of drones due to mobility and limited power supply. A drone low in power might be turned off until it is recharged, during which time the associated fog capabilities are lost and may need to be accommodated by other drones. A drone flying away from some area may look for a replacement to continue the ongoing service in this area. Therefore, in addition to tracking drones in-service, the coordination algorithms require tracking of drones in other states, e.g. available (but not in-service), partially in-service, etc. This results in a coordination scheme which not only associates drones into a cluster but also adapts to the dynamic capability distribution within the group.

5.2.3.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.27.

5.2.3.3 Actors

- ***[Machine]:*** Fog Node: A fog node is a node with certain types of fog capabilities or resources such as computing, storage, control, networking, that can be shared with and leveraged by users and other fog nodes. A fog node may have one or multiple types of capabilities, may also have other software or services that are running on the node. A fog node can be located at the edge of deployment or higher layers. The fog nodes, especially the ones close to the edge, are considered to have limited capabilities compared to the cloud, and the capabilities may not be available all the time.

- ***[Machine]:*** Fog Leader: Fog leader is a fog node that will coordinate and combine other fog nodes together to serve a fog service request which demands large fog capabilities and cannot be completed at a single fog node. A fog leader will form both potential group(s) for fog capability discovery, and service group(s) for serving fog service requests. The fog leader could be located at any layer of the fog hierarchy, as long as it is capable of forming potential groups, creating service groups, and adjusting service groups.

- ***[Human]:*** User/Requestor: A user/requestor is the entity that may send a fog service request to the fog leader. The request may ask for completing a task, reserving capabilities for a period of time or consistently providing fog service.

- ***[Machine]: IoT Service Layer Platform:*** The Service layer platform identifies fog nodes that can cooperate to complete a request and to track their capabilities (e.g. battery level, available memory) in an efficient manner. It can select a group of fog nodes to cooperate on a fog service request and split the request into multiple sub-requests according to the type, amount, and availability of the selected fog nodes' capabilities, such that the capability requirement in each sub-request will not exceed the capacity of the corresponding fog node. It can coordinate a group/cluster of fog nodes to provide services to a user. It can cooperate on a service to re-allocate tasks among the group nodes as needed to adapt to the dynamic capability distribution within the group. It can identify and manage hierarchical fog clusters.

- **Data user/consumer:** Drone in role of Fog Node, Drone in Role of Fog Leader, User/Requestor of Fog services, IoT Service Layer Platform.

5.2.3.4 Pre-conditions

- Fog nodes are deployed, each willing to share (part of) its fog capabilities.

- Fog nodes may have discovered nearby (geographically or logically) fog nodes.

- At least one fog node is willing and capable to act as the fog leader to coordinate several fog nodes in completing a request.

5.2.3.5 Triggers

- A (potential) fog service request requires multiple fog nodes' capabilities to fulfil.
- The capability of a fog node changes.
- A new fog node enters the coverage of a fog leader, or a fog node leaves the coverage of a fog leader.

5.2.3.6 Normal Flow

Figure 5.2.3.6-1 illustrates the high-level flows of cooperative fog service use case, which consists of the following steps:

- Step 1: The fog leader may discover capabilities of fog nodes that can potentially cooperate on a future fog service request. The capability of a fog node may include computing (with CPU resource), storage (with memory resource), communication (with bandwidth resource), sensing, controlling, actuating (with firmware or software resource), etc. The fog leader may track the status of the potential fog nodes as well as their capabilities, which may later be used as the reference or hints when selecting nodes to complete a fog service request.
- Step 2: The user sends a fog service request to the fog leader. The request may ask for a certain number of resources (e.g. 1 GB data storage) to be reserved for a period of time, or to complete a task with or without a completion time constraint (e.g. perform data analysis on the video data generated from equipped cameras (within 5 minutes)), or to provide consistent service (e.g. monitor the traffic density of the downtown area and calculate optimal path).
- Step 3: Based on the received request, the fog leader selects a group of fog nodes and reserves capabilities from the nodes for the request.
- Step 3.1: After receiving a request, the fog leader will first interpret the request to get information of what and how much capabilities are required, and select fog nodes to satisfy the requirements. Based on that, the request will be split into sub-requests for each selected fog node with each containing a relatively small portion of capability requirements such that they can be handled by the fog nodes cooperatively. For example, the request may ask the drones to monitor the environment in a large area, while each drone can only cover a small area. In this case, the request will be divided into sub-requests with each one corresponding to a sub-area covered by one drone, and the leader will then merge the results collected from the drones to complete the request. Moreover, the request may ask for a storage size or computation speed that exceeds the capacity of a drone, in this case the request can be sliced into "smaller" sub-requests and jointly completed by multiple drones. The request can also be split in the time domain according to the predicted availability of fog nodes in case some fog nodes are only available for a limited period of time. For example, a 24-hour surveillance request can be split into daytime and night-time sub-requests and assigned to different sets of drones, where the day-time working drones will be turned off for recharging during night-time and their place taken by the night-time working drones.
- Step 3.2: After splitting, the sub-requests will be distributed to the selected group of fog nodes along with the capability requirements for each fog node.
- Step 3.3: The fog nodes reserve capabilities according to the received sub-requests.
- Step 3.4: After reserving the required capabilities, the fog nodes send responses to the fog leader indicating whether the reservation is successful.
- Step 4: The fog leader sends a response to the user indicating whether the request can be completed.
- Step 5: Under the coordination of the fog leader, the group of selected fog nodes will provide fog service with the reserved capabilities, or the user will start to use the fog services provided by the fog nodes. Dynamics or changes during this step may trigger service update in the next step.

- Step 6: The capabilities of the in-service fog nodes may be changing and result in group dynamics. The update of fog service request, receiving multiple requests competing for the same fog node's capabilities, or a time sequential request may also trigger the group dynamics since the leader will need to make adjustments to the group to adapt to the changes. As such, the fog leader needs to perform dynamic group management or service update accordingly.

- Step 7: After the fog request is completed or the subscription/lease of fog capabilities terminates, the reserved fog capabilities will be released.

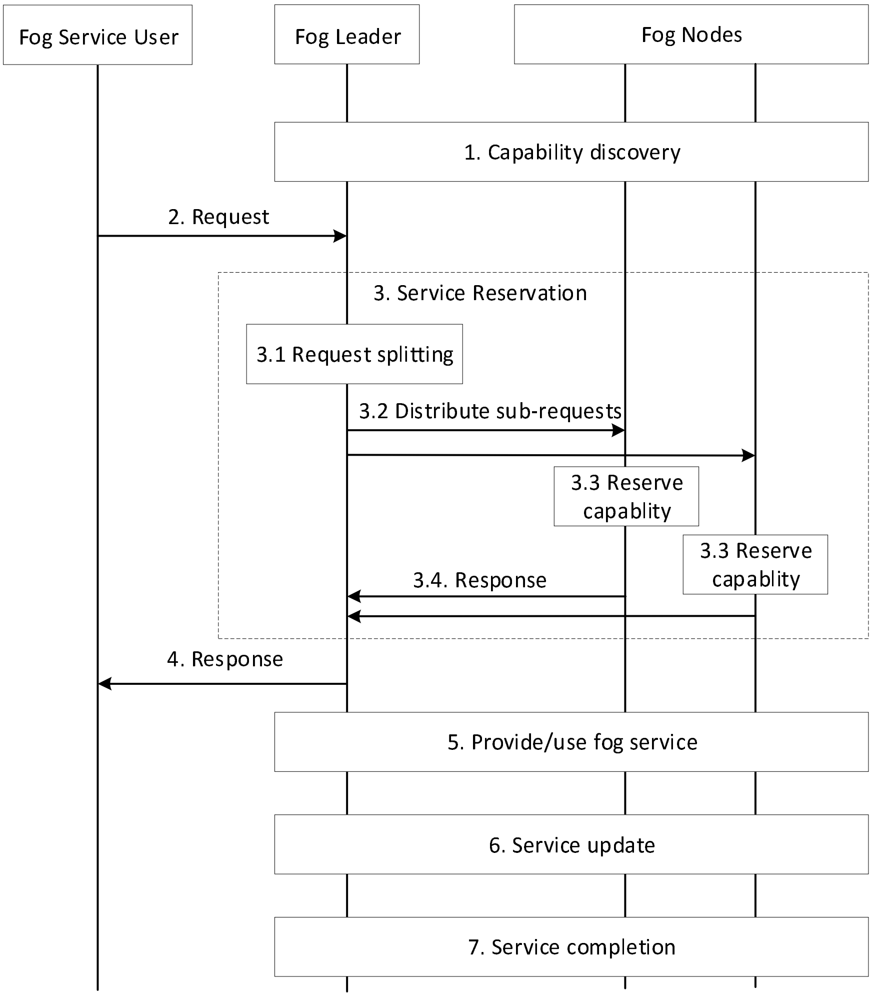

Figure 5.2.3.6-1: Normal Flow - Cooperative fog service

5.2.3.7 Alternative Flow

None.

5.2.3.8 Post-conditions

None

5.2.3.9 High Level Illustration

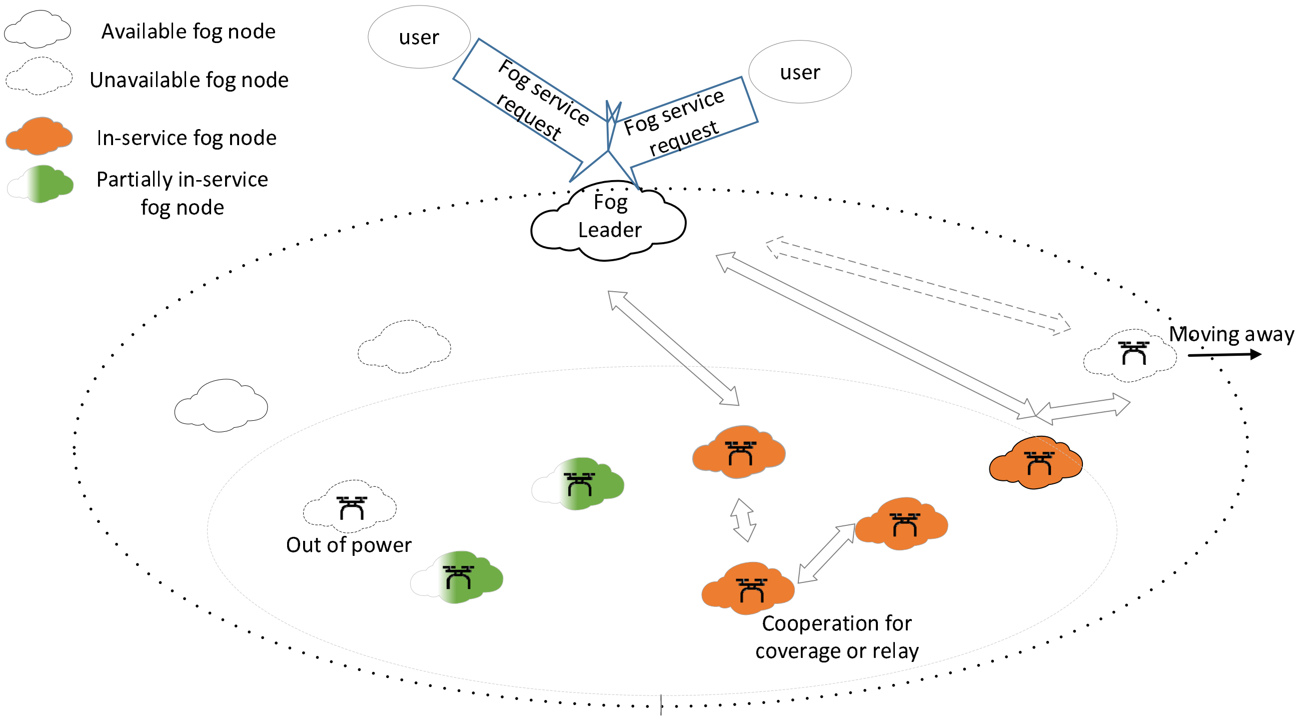

Figure 5.2.3.9-1: High Level Illustration - Cooperative Fog Service

5.2.3.10 Use case analysis

IoT data that may compromise data usability:

- Capabilities of a Fog node: when a device is included in the Fog, if it does not describe its capabilities correctly then the overall service requests cannot be handled optimally.

- Status of a Fog node: When reporting status, if the status is not described then the overall "user service request" cannot be completed.

- Fog node commands: when a device is commanded to perform a service, if the command is not recognized then the node may not be efficiently utilized.

5.3 Industry and Manufacturing Use Case

5.3.1 Use Case C.1: Monitoring of industrial manufacturing equipment

5.3.1.1 Description

A common application of Artificial intelligence in industry and manufacturing is the improvement or optimization of machinery used for production, construction, and/or delivery.

5.3.1.2 Source

Derived from various articles.

5.3.1.3 Actors

The presence of the following actors/entities as well as their associated roles are envisaged in the current Use Case:

- ***[Machine]:*** Machinery, equipment or vehicles that have normal operating parameters.
- ***[Device]:*** sensors that measure some aspect of the equipment.
- ***[Machine]:*** AI/ML processing of sensor data.
- ***[Human]:*** A monitor, human or automatic, that can react based on the measured operating conditions of the equipment and/or the signals/indicators from the AI/ML processing.
- **Data user/consumer:** The monitor, human or automatic.

5.3.1.4 Pre-conditions

Equipment is operating in order to accomplish some task. Examples can be motors or electronics that generate heat or vibrations that can be measured with sensors. There exists an understanding of normal operating conditions, or the equipment is currently operating normally.

5.3.1.5 Triggers

The sensors measure aspects of the equipment that start to operate outside of normal parameters.

5.3.1.6 Normal flow

Machinery or equipment operate according to their designed purpose. The sensors measure aspects of the machinery or equipment operating parameters. The AI/ML algorithm processes data from the sensors to detect and identify when the equipment is operating outside of normal parameters. When the measured parameters of the equipment go outside the "normal" range, a signal or indicator is generated for the system operators to act upon to get the equipment back into normal operating range.

5.3.1.7 Alternative flow

The AI/ML algorithm identifies that the sensors are not operating within normal parameters.

5.3.1.8 Post-conditions

An irregular operating condition has been detected and signalled to a monitor that was able to take appropriate action based on the detected anomaly.

5.3.1.9 High Level Illustration

N/A.

5.3.1.10 Use case analysis

Data that may compromise data usability: data coming from the sensors.

If data are not generated normally (at the expected time intervals) or corrupted (fail to detect abnormal conditions), there is a risk that the machinery comprising the industrial production line could be damaged or the product that would be generated would be defective.

5.3.2 Use Case C.2: Monitoring of industrial manufacturing products

5.3.2.1 Description

A common application of Artificial intelligence in Industry and manufacturing is the detection of flaws in the manufacture of a product. For example, a process that produces canned food may detect that a label was not properly applied to the can or a damaged can. This can occur in a variety of stages, for example "can" manufacture, labelling, packaging in cartons for shipping, loading cartons onto transportation, stocking products in retail stores, delivery from delivery services.

5.3.2.2 Source

Derived from various articles.

5.3.2.3 Actors

The presence of the following actors/entities as well as their associated roles are envisaged in the current use case:

- ***[Device]:*** sensors that can identify an aspect of a product that is not correct (visual, weight, structural integrity).
- ***[Device]:*** AI/ML processing of sensor data.
- ***[Human]:*** A monitor, human or automatic, that can react based on the detected anomaly of a product being manufactured or some other part of a repetitive process.
- **Data user/consumer:** A monitor, human or automatic.

5.3.2.4 Pre-conditions

Products are being produced in an assembly line type of process. There exists an understanding of characteristics of the products in the stage being evaluated.

5.3.2.5 Triggers

The sensors measure aspects of the product being evaluated and identify an anomaly.

5.3.2.6 Normal flow

Products are being manufactured or moved within a supply chain process. The sensors measure aspects of the products. The AI/ML algorithm processes data from the sensors to detect characteristics of a product that are outside normal parameters. When characteristics of the product go outside the "normal" range, a signal or indicator is generated for the system operators to act upon to take an appropriate action.

5.3.2.7 Alternative flow

The AI/ML algorithm identifies that the sensors are not operating within normal parameters.

5.3.2.8 Post-conditions

Products that are not normal are detected and identified and sensors are operating within normal parameters.

5.3.2.9 High Level Illustration

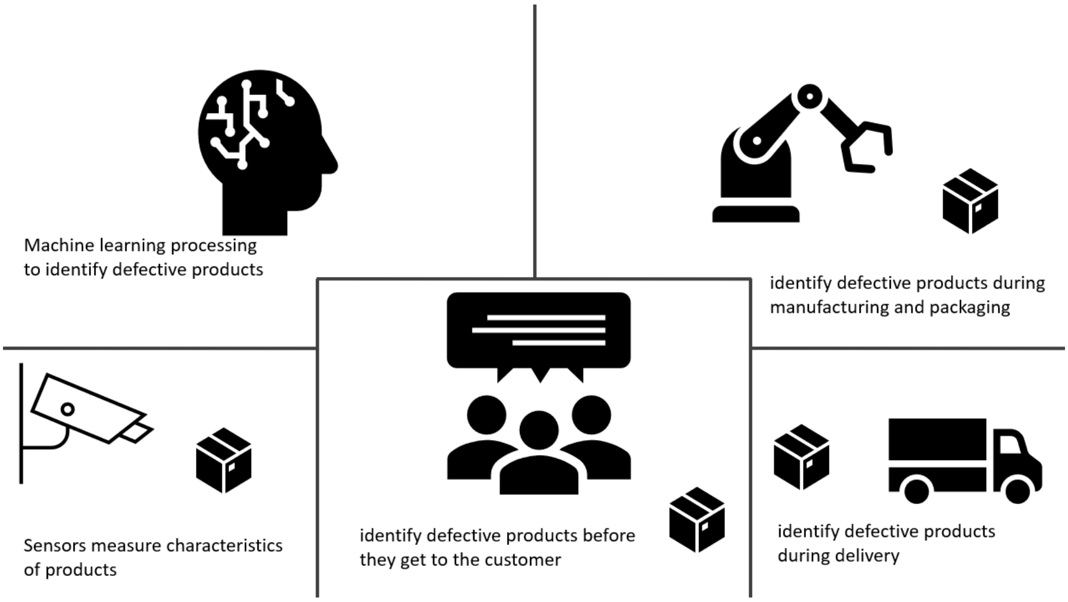
Machine learning processing
to identify defective products
identify defective products during
manufacturing and packaging
Sensors measure characteristics
of products
identify defective products before
they get to the customer
identify defective products
during delivery

Figure 5.3.2.9-1: High Level Illustration of industrial Manufacturing Products

5.3.2.10 Use case analysis

Data that may compromise data usability: sensor data.

This could result in defective products provided to consumers (for example, a bag of chips is not fully closed).

5.3.3 Use Case C.3: Link Binding in Digital Twins and Edge/Fog Computing

5.3.3.1 Description

In a smart manufacturing use case in emerging Industry 4.0 and/or Industrial Internet, physical domain and cyber domain are connected via Internet technologies toward industrial Cyber-Physical Systems. Various sensors and actuators will be installed and/or attached to physical parts, machines, and devices in the physical domain so that their status and information will be effectively collected to the cyber domain or the Internet. On the other hand, reverse control commands may be issued from the cyber domain to a single physical part, machines, and/or devices. Smart manufacturing in general aims to render the manufacturing process more efficient, autonomous, and smart by leveraging Internet of Things (IoT) and the convergence of Information Technology (IT) and Operation Technology (OT) in product lifecycle.

To exploit the full range of benefits from smart manufacturing, the concept "digital twins" has been proposed. Basically, digital twins refer to digital or virtual companions of physical products; digital twins use collected data from sensors installed on physical products to represent their near real-time status, working condition, and/or other information. Through digital twins, a physical product can be monitored, managed, and maintained remotely and even more efficiently without sending any technician to check the product physically. Digital twins actually necessitate link binding and resulted automatic content synchronization from physical products to their digital twins or vice versa.

5.3.3.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5].

5.3.3.3 Actors

- ***[Machine]:*** Source Resource Host: A logical entity which hosts source resources.
- ***[Machine]:*** Destination Resource Host: A logical entity which hosts destination resources.

- ***[Machine]:*** Link Binding Coordinator A logical entity or a management application which manages link bindings between source resources and destination resources.
- ***[Machine]:*** Resource Creator: A logical entity which creates source resources at destination resource.
- **Data user/consumer:** Resource Creator (logical entity).

5.3.3.4 Pre-conditions

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.22.

5.3.3.5 Triggers

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.22.

5.3.3.6 Normal flow

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.22.

5.3.3.7 Alternative flow

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.22.

5.3.3.8 Post-conditions

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.22.

5.3.3.9 High Level Illustration

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.22.

5.3.3.10 Use case analysis

Data that may compromise data usability: sensor data.

Sensors and Actuators attached to collect data in Physical part to create digital twin is corrupted either by link breaking or data collected is incorrect as a result of fault in sensors. These may result in wrong representation of physical product in digital form in real time as such the product is not being monitored or managed remotely. In situation where the product being manufactured is sensitive food, or children's toys this may lead to faulty batches that may compromise safety and lead to recall of product which may prove expensive.

5.4 ICT Network Management

5.4.1 Use Case D.1: Intelligent Software Rollouts

5.4.1.1 Description

With an intelligent software roll out, although automatic, the wrong data can have consequences on the system and this use case reviews such use and the effect. Physical resources such as routers, during their lifetime, need to have their firmware updated, not only for the support of new services or functionalities, but also to fix existent impairments. In some cases, a firmware rollout can take several months to plan and enforce. By making use of the Experiential Networked Intelligence (ENI) System, operators can define different policies for different types of rollouts and for different types of resources. One example could be the definition of a hierarchy of parameters for phasing out the rollout, e.g. client class, geographical location, or time of the day. In addition, and also taking dynamic on boarding and DevOps environments into consideration, different types of policies can be defined by using the ENI System, such as:

- Development, e.g. tests should provide a correlation between network function performance (throughput, jitter, delay) and resource utilization (CPU, RAM, I/O).

- Update schedule, e.g. for enterprise customers schedule updates outside business hours.
- Update procedures, e.g. create backup of current versions of software instances when updating instances from platinum level services in order to prevent service disruption in case of occurrence of significant errors.
- Failure procedures, e.g. considering two types of errors where the response would be defined by policies: minor errors, which makes the ENI System retry the update. Thus, the use of AI methods becomes more important when moving software from testing to production by using automatized procedures.

5.4.1.2 Source

Derived from ETSI GR ENI 001 use case in clause 5.3.3 [i.6].

5.4.1.3 Actors

The presence of the following actors/entities as well as their associated roles are envisaged in the current Use Case:

- ***[Human]*** Customers/clients: the operators themselves.
- ***[Human]*** Network Administrator: entity/person responsible for the initial policy design that encompasses the definition of different activities during rollouts.
- ***[Machine]*** Network Infrastructure (Routers): infrastructure that includes resources that are meant to be upgraded or, in the worst case, replaced, these have the sensors that send the signal of its current status used to determine if an update is needed.
- ***[Machine]*** ENI System: system solution that makes use of AI methods when upgrading or moving software from testing to production, and that enables the use of policies to govern updates to software instances. This solution also participates in software tests and builds a profile with information, e.g. correlation between network function performance (throughput, jitter, delay) and resource utilization (CPU, RAM, I/O), that can be used to improve fulfilment and assurance procedures.
- ***[Machine]*** OSS/BSS: operational and business systems that belong to the management system of network operators. In this case they are providing, among others, monitoring, actuation, internal records of very different items that may range from products to resources, as well as other business interfaces dedicated to external entities.
- **Data user/consumer:** ENI system automation.

5.4.1.4 Pre-conditions

The network is operating in perfect conditions with all its components in good shape. Moreover, the network operator already has a development environment that is specified to mimic the production environment. This development environment is used to run automatized tests in order to validate new software versions and build the respective software profile, where the series of tests are defined by network operator policies. Finally, the move of software from development to a production environment is also conditioned by network operator policies, thus governing the phased deployment of the new version.

5.4.1.5 Triggers

A new software version of a virtual component is released by the vendor and is on boarded on a network operator infrastructure. The upload of a new software version to software repository triggers the start of automatic tests pre-defined by policies also previously enforced in the ENI System.

5.4.1.6 Normal flow

The following sequence of actions may be identified:

1) A new software version is instantiated on the network operator development environment.
2) Within the new environment, the software is subject to a series of tests determined by pre-defined policies in the ENI System, which results, will be used to create a software profile.

3) During the tests, the ENI System starts analysing the behaviour of all the collected data from the devices such as the version of software on the computers, and compares it with the profile of previous versions of software.

4) Since the results of the tests are conformant to previous versions, the ENI System is in position to allow the triggers for moving the new version from the development to the production environment.

5) The ENI System takes into account the pre-defined operator policies for the new software rollout and performs the scheduling of updates for the software instances.

6) The ENI System triggers the movement of the new version from the development to the production environment.

7) During the update, all platinum SLA customers of software instances are using a redundant software instance to avoid any service disruption.

8) Some instances monitoring data may detect an inconsistency with the application profile indicating a problem with the update. Since it is considered a minor error, the ENI System retries the update on failed instances.

9) At the end of the process, the ENI System may notify relevant software components, e.g. OSS/BSS, that the software rollout has been carried out successfully.

5.4.1.7 Alternative flow

None.

5.4.1.8 Post-conditions

The new software version has been updated on all deployed instances and inventories. The network and corresponding services are running steady.

5.4.1.9 High Level Illustration

None.

5.4.1.10 Use case analysis

Data that may compromise data usability: report of the updating process.

User intervention may interrupt the automatic software update. Monitoring of data generated by sensors may produce inconsistency of results which may affect the retries of failed upgrade. Also forces user intervention whilst update is taking place may give false feedback that installation has been completed which may not be the case. The consequence of update not happening means that the software was not fully deployed properly and this is not detected, this suggests inconsistencies in all system and could mean unfruitful use of resources indirectly financial implication to organization.

5.4.2 Use Case D.2: Policy-based network slicing for IoT security

5.4.2.1 Description

In the near future, it is expected that smart cities will be built by using a myriad of IoT devices, where a significant number of them will be connected through 5G. These devices will play a vital role in the deployment of various services (e.g. civil protection or other services provided by the municipality, where each service will have its own target use and different device requirements).

To support this massive deployment of devices, the use of network slices will enable their aggregation either by functionality (e.g. security or city operations management support) or by other types of lower level requirements, such as low latency and high bandwidth.

In this context, the handling of Distributed Denial Of Service (DDOS) attacks plays a crucial role as those devices are usually meant to be part of the support to applications/services related to social interest.

One use of machine learning in the ENI System is to detect specific traffic patterns indicating DDOS or other type of attacks. This is because the increasing sophistication of such attacks makes it harder to use simpler algorithms (e.g. pattern recognition) that focus on a set of predefined information. The symptoms of a DDOS attack include unusually slow network performance and/or the inability to access a particular set of web sites. When this happens, the ENI System will be able to detect and learn from the occurrence by using AI methods. If the new traffic pattern is identified as an attack based on past history, the ENI System will be able to trigger appropriate responses from the related management components. In addition, AI enables different types of attacks to be correlated. For example, different attacks could use different protocols, but all be directed at the same target. This type of conclusion is extremely hard to make without using inferencing.

By using those techniques, the ENI System will be able to identify these and other types of attacks with a shorter timeframe and better precision when compared to today's systems.

5.4.2.2 Source

Derived from ETSI GR ENI 001 [i.6], use case in clause 5.1.

5.4.2.3 Actors

The presence of the following actors/entities as well as their associated roles are envisaged in the current Use Case:

- ***[Human]*** Customers/clients: the operators themselves.
- ***[Machine]*** Network Infrastructure: infrastructure that includes resources and devices that are meant to provide applications/services related to social interest.
- ***[Device]*** IoT devices: normal devices and infected devices, e.g. those that are victims of a Botnet malware attack.
- ***[Human]*** Network Administrator: entity/person responsible for the policy design that encompasses the isolation of devices that were victims of DDOS attacks.
- ***[Machine]*** OSS/BSS: components that provide monitoring data slicing management functionalities for ENI to detect and mitigate attacks. In addition, they also provide interfaces to network administrators and customers.
- ***[Machine]*** ENI System: System solution that makes use of AI methods to identify and trigger responses to attacks.
- **Data user/consumer:** ENI system automatic.

5.4.2.4 Pre-conditions

The network is operating correctly.

5.4.2.5 Triggers

Derived from ETSI GR ENI 001 [i.6], use case in clause 5.1.

5.4.2.6 Normal flow

Derived from ETSI GR ENI 001 [i.6], use case in clause 5.1.

5.4.2.7 Alternative flow

N/A.

5.4.2.8 Post-conditions

Derived from ETSI GR ENI 001 [i.6], use case in clause 5.1.

5.4.2.9 High Level Illustration

N/A.

5.4.2.10 Use case analysis

Data that may compromise data usability: ENI monitoring data.

Potential error is if the ENI data collected from the websites or devices for example are corrupted in some way which means that the ENI system is unable to detect that abnormal event has occurred (e.g. web site is no longer accessible, or the traffic patterns of a device do not correspond to its expected behaviour) and unable to carry out necessary analysis that determines if system is under attack or not.

Data collected from devices should be available to the Network Administrator before analysis so if required there can be an intervention from the Network Administrator based on their own analysis.

5.4.3 Use Case D.3: Personal data management mechanism based on user's privacy preference

5.4.3.1 Description

The data collected by the M2M platforms may include personal information or sensitive information of data providers, hence, the access to such data should be controlled appropriately. This use case shows the data management mechanism based on data provider's privacy preferences, which is developed as a PPM (Privacy Policy Manager). The access from application service providers to the collected data at M2M service platform is controlled based on the privacy preferences that are configured by the data providers, unnecessary and unwanted access to the collected data is blocked appropriately.

5.4.3.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5].

5.4.3.3 Actors

The presence of the following actors/entities in the current Use Case:

- ***[Machine]:*** Front-end data-collection equipment (M2M devices).
- ***[Machine]:*** Management platform (M2M Service Provider's Platform).
- ***[Human]:*** Data provider.
- ***[Device]:*** PPM: A PPM function manages privacy preferences of the data providers.
- ***[Human]:*** Application service providers: This actor provides many kinds of services to service users.
- **Data user/consumer:** Application Service Providers.

5.4.3.4 Pre-conditions

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12:16.

5.4.3.5 Triggers

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.16.

5.4.3.6 Normal flow

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.16.

5.4.3.7 Alternative flow

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.16.

5.4.3.8 Post-conditions

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.16.

5.4.3.9 High Level Illustration

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.16.

5.4.3.10 Use case analysis

Data that may compromise data usability: report of the updating process.

The consequence of data not been usable means the data provided is incomplete when preference data is being configured in the PPM. It could also mean that during configuration of preferences that, connection is lost which leads to the data provided to the PPM for use by the Application Providers is compromise and this may lead to the wrong service being provided to the user resulting in misrepresentation of service of user data is compromised.

5.4.4 Use Case D.4: Collection of M2M System data

5.4.4.1 Description

M2M Service Providers have a need to provide the Application Service Providers with data and analysis related to the behaviour of the M2M System as well as the service provider supplied components of the M2M System (e.g. Device Gateway) M2M Operators face two problems. M2M Service Providers can utilize the methods of Big Data by collecting M2M System data for the behaviour of the M2M System as well as data from M2M System components provided by the Service Provider. In this scenario, the data is collected from M2M Gateways and Devices provided by the M2M Service Provider. The M2M System data that is collected from the M2M Devices and Gateways can be described as:

- M2M System Behaviour.
- Component Properties.

M2M System Behaviour: Data related to the operation of the M2M Applications within the M2M System. Types of data that is to be collected includes information related messages transmittal and reception (e.g. bytes, response times, event time). Component Properties: Data related to the Service Provider supplied components as the component is in use by the M2M System (e.g. location, speed of the component, other anonymous data).

With this data, the M2M Service Provide can provide:

1) Analysis of the data without knowledge of content of the Application's data.
2) Insights into the operation of the M2M Applications. For example, the M2M Service Provider can infer the "correct" state of the application, or the network status changes, by the analysis of the data, and then trigger some kinds of optimization mechanisms.

5.4.4.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 12.6.

5.4.4.3 Actors

- ***[Machine]:*** Front-end data-collection equipment (e.g. M2M Devices and Gateways).
- ***[Machine]:*** Management Platform (e.g. M2M Service Provider's Platform).
- ***[Human]:*** Monitor Centre (e.g. M2M Application's Platform).

- ***[Machine]:*** M2M System Data Collection Centre.
- **Data User/consumer:** Management platform, Monitor Centre, Data collection centre.

5.4.4.4 Pre-conditions

None.

5.4.4.5 Triggers

- Time trigger: collecting data at a specific time.
- Position trigger: collecting data when position changed.
- Behaviour trigger: collecting data when certain behaviour happened.

5.4.4.6 Normal Flow

1) The M2M Device and Gateway collects M2M System data.

2) Once a trigger is activated, the M2M Devices and Gateway sends the M2M System data to the M2M System Data Collection Centre.

5.4.4.7 Alternative Flow

None.

5.4.4.8 Post-conditions

None

5.4.4.9 High Level Illustration

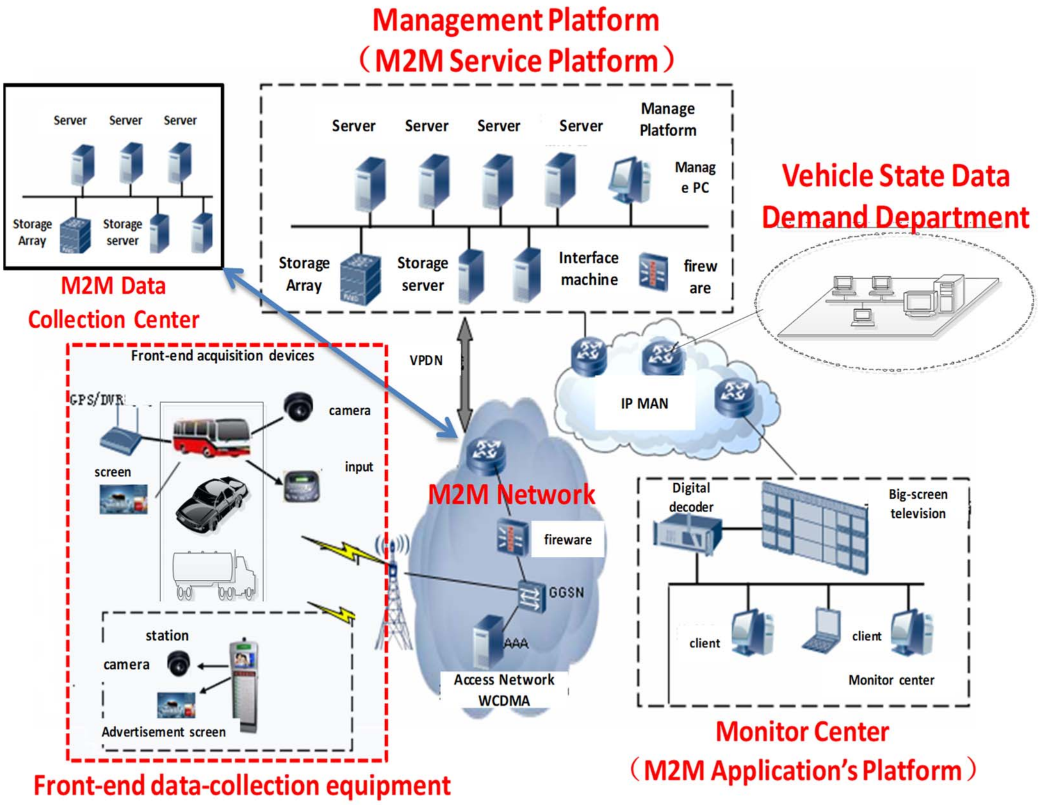

Figure 5.4.4.9-1: Vehicle Operation Management System

The vehicle operation management system depicted in Figure 5.4.4.9-1 is an exemplary use case for the collection of M2M system data.

- Vehicle Operation Management System provide users a new telecommunications business with remote collection, transmission, storage, processing of the image and alarm signals.

- Front-End Data Collection Equipment include Front-End 3G camera, Electronic Station, Car DVR, costumed car GPS, WCDMA wireless routers and other equipment.

- Management Platform with business management function, include:

  - Forwarding, distribution, or storage of images.

  - Linkage process of alarms.

  - Management and maintenance of the vehicle status data.

- Monitor Centre: consists of TV wall, soft/hardware decoder, monitor software, etc.

- Vehicle State Data Demand Department: such as auto shop, vehicle repair shop, vehicle management centre, automobile and parts manufacturers, government regulatory platform, etc.

- M2M System Data Collection Centre: use built-in data collectors resided in Network Equipment, M2M Platform, Costumed M2M Modules and Costumed M2M Terminal Devices to collect M2M System data.

5.4.4.10 Use case analysis

IoT data that may compromise data usability:

Format and meaning of the Metric data provided to a M2M System Data Collection Centre has to be "understandable". If the information is not consistent there could be incorrect "insights" provided. For example, timestamps should have a defined and understandable format.

If metric data is not properly defined and generated by the M2M System the analysis of the data may not be consistent and analysis of the data can be impacted. An example could be a query that asks how many devices can a M2M system support without degradation, where the answer can depend on how much traffic the devices generate, the size of each message, the complexity of the service layer function being used and the number of nodes that are traversed to reach the target M2M System.

5.5 Agriculture and Farming

5.5.1 Use Case E.1: Fertilization/Irrigation/Pest management service

5.5.1.1 Description

This use case relates to a technological solution offering a range of innovative smart farming services that provides next generation advice to farmers. Such a technological solution is offered as an inexpensive service with zero technological related investment for farmers, making it accessible even to small farmers.

The system consists of an infrastructure of IoT devices, a set of cloud computing services, and a set of smart farming advisory services.

IoT devices work as telemetric autonomous stations which collect data from sensors installed in the field and record atmospheric (air temperature, relative moisture, wind direction and velocity, rain, leaf wetness) and soil parameters (temperature, moisture) and control irrigation systems.

The cloud service combines the data collected from IoTs with data from other sources (i.e. weather forecast services and satellite images) and converts them into facts using advanced data analytic techniques. The embedded Decision Support System (DSS) transforms facts into an initial advice, which is accessible to farmers through the apps and certified agricultural advisors, which are employed by third-parties. The advisors are reviewing and evaluating the given information for providing the final advice and support to the farmers.

The advising and supporting services that are provided by the combination of the software and certified advisors, which provides Fertilization and Irrigation advice, as well as Pest Management/Hazard warnings.

5.5.1.2 Source

Internet of Farming H2020 project (IoF2020 - Grant number 731884): [i.4].

5.5.1.3 Actors

- ***[Human]:*** Farmers, which can automatically monitor the status of all sensors and to exploit the analysis of provided data for optimizing the fertilization and irrigation system.

- ***[Device]:*** IoT devices network, which is in charge of measuring environmental information and to send them to the Decision Support System.

- ***[Machine]:*** Decision Support System, which is in charge of collecting all the data and analyse them.

- **Data user/consumer:** Decision support system, Farmers.

5.5.1.4 Pre-conditions

- The IoT devices, the cloud services and the decision support system are deployed and in operational condition.

- The data collection services are up and running.

5.5.1.5 Triggers

- The decision support system inferred specific advices for managing the irrigation and fertilization system.

5.5.1.6 Normal flow

- The sensors register environmental data and send them to the cloud service.
- The cloud service collects all the data provided by the sensors and save them into the internal knowledge graph.
- The decision support system processes in real-time the new data stored into the knowledge graph and generates actions that are suggested to farmers together with the motivations driven such recommendations.
- Farmers check if the system set the fertilization and irrigation system properly and/or if some issues related to the pest management have been detected.

5.5.1.7 Alternative flow

None.

5.5.1.8 Post-conditions

The fertilization and irrigation system is calibrated properly.

5.5.1.9 High Level Illustration

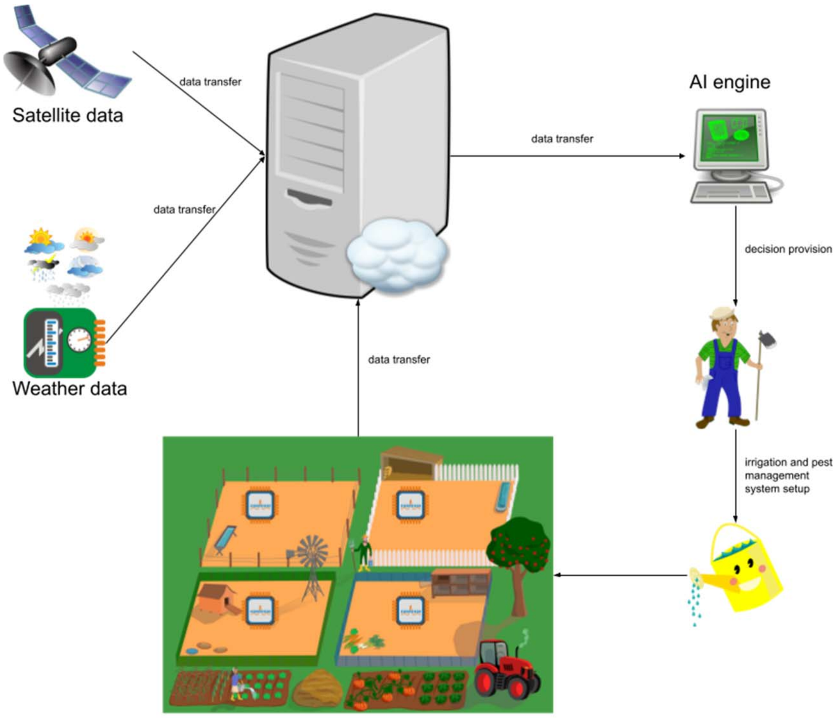

Figure 5.5.1.9-1: High level illustration of Smart Agriculture Fertilization/Irrigation/Pest management service use case

5.5.1.10 Use case analysis

Data that may compromise data usability:

- Data provided by the satellite.
- Data provided by weather stations.
- Device and IoT data located in the field.

The decision support system is driven by the three types of data mentioned above. If one of the data sources fails to read the values or to provide them promptly, they would become not usable by the system with the risk of having an ineffective management of the farming system.

In particular, the IoT devices located in the field are particularly exposed to adverse events (e.g. meteorological ones). This aspect can be mitigated by implementing a redundant network of sensors that can be used both as backup or as confirmation of the read values. This action would increase the overall data usability.

5.6 Mobility (Transportation) use cases

5.6.1 Use Case F.1: Vehicle Diagnostic & Maintenance Report

5.6.1.1 Description

The Vehicle Service Centre wants to help the vehicle owner to be aware of the status of the vehicle and remind them to maintain the vehicle in a timely manner to avoid any damages.

Hence the Vehicle Service Centre needs to obtain and analyse data from the vehicle periodically. Based on the analysis result, it will notify to the vehicle owner showing what's going on with the vehicle, in simple language and images together with some maintenance suggestions.

More specific examples of this use case have been defined by the ASSIST-IoT project in their deliverable [i.22] (see also clause 5.6.3 for more information about the ASSIST-IoT project):

- Fleet in-service emission verification: emission regulations for propulsion systems are getting stricter globally. This sub use case allows to prove the vehicles' emission conformity while the fleet is in service, throughout the vehicles' lifetime and, possibly, under real driving scenarios. Instead of conducting discrete tests on a sample of individual vehicles, the focus is moved to the emissions distribution of the entire fleet (ISE, In-Service Emissions), smoothing extreme scenarios for which a single test may fail all the time, but are potentially irrelevant from a statistical point of view.
- Vehicle diagnostics and non-conformance causes identification: a potentially defective vehicle is placed under active monitoring and is diagnosed using intelligent methods that are updated on demand.
- Vehicle exterior condition inspection and documentation: this service scans a vehicle and documents the condition of its exterior. It is complemented by the exterior defects detection support service which verifies the information that was recorded by the vehicle scanner and identifies any defects with support from the IoT system while visually inspecting the vehicle.

5.6.1.2 Source

oneM2M TR-0026 [i.10], use case in clause 6.1.

"Use Cases Manual & Requirements and Business Analysis - Initial", Assist-IoT project report [i.22].

5.6.1.3 Actors

- ***[Device]:*** M2M Device: It is embedded in a vehicle, which is used to send information to Vehicle Service Centre and implements diagnostics function from Vehicle Service Centre.

- ***[Machine]:*** Vehicle Service Centre: It operates a service platform for diagnostics and maintenance of vehicles, obtains and analyses the diagnostics data from the vehicle. It will also send the vehicle Diagnostic & Maintenance Report together with maintenance suggestions to the vehicle owner.
- ***[Human]:*** Vehicle Owner: By reading the Vehicle Diagnostic & Maintenance Report sent from the Vehicle Service Centre, the vehicle owner can decide whether to maintain his/her vehicle.
- ***[Human]:*** Vehicle Service Centre technician: He receives information about vehicle defects by direct contact with the vehicle owner, reads out data from vehicle to support fault investigation, performs further maintenance and diagnostics tasks, orders defect parts after they have been identified. He may also provide feedback to the manufacturer about vehicle issues that were discovered while in garage.
- **Data user/consumer:** Vehicle Owner, Vehicle Service Centre, Vehicle Detection M2M Application, Vehicle Service Centre technician.

5.6.1.4 Pre-conditions

See oneM2M TR-0026 [i.10], clause 6.1 and Assist-IoT deliverable [i.22], section 5.

5.6.1.5 Triggers

See oneM2M TR-0026 [i.10], clause 6.1 and Assist-IoT deliverable [i.22], section 5.

5.6.1.6 Normal flow

See oneM2M TR-0026 [i.10], clause 6.1 and Assist-IoT deliverable [i.22], section 5.

5.6.1.7 Alternative flow

See oneM2M TR-0026 [i.10], clause 6.1 and Assist-IoT deliverable [i.22], section 5.

5.6.1.8 Post-conditions

See oneM2M TR-0026 [i.10], clause 6.1 and Assist-IoT deliverable [i.22], section 5.

5.6.1.9 High Level Illustration

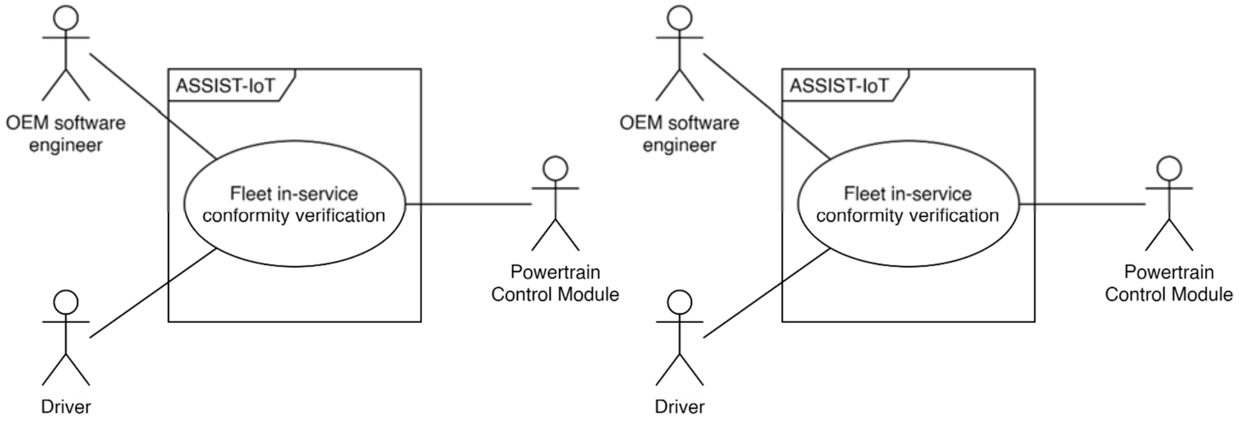
OEM software engineer
ASSIST-IoT
Fleet in-service conformity verification
Powertrain Control Module
Driver
OEM software engineer
ASSIST-IoT
Fleet in-service conformity verification
Powertrain Control Module
Driver

Figure 5.6.1.9-1: Illustration of fleet in-service emission verification

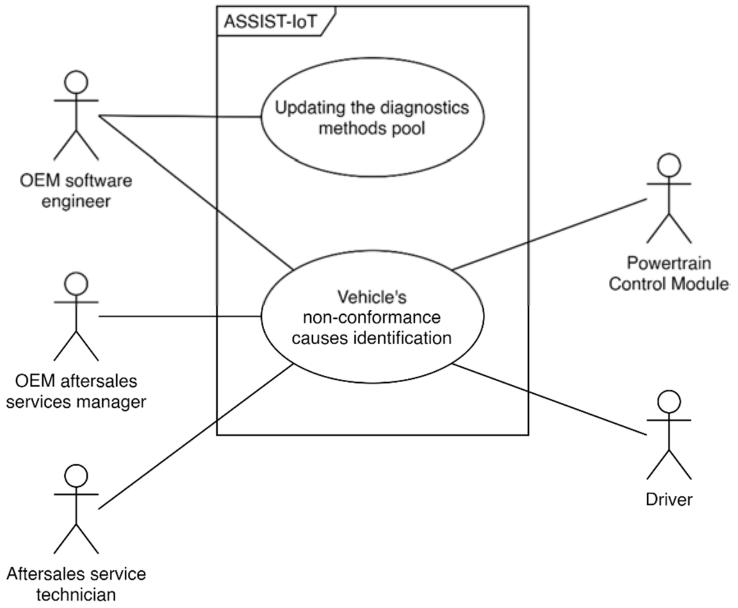
ASSIST-IoT
Updating the diagnostics methods pool
OEM software engineer
Powertrain Control Module
Vehicle's non-conformance causes identification
OEM aftersales services manager
Driver
Aftersales service technician

Figure 5.6.1.9-2: Illustration of vehicle's non-conformance causes identification and diagnostics methods pool update

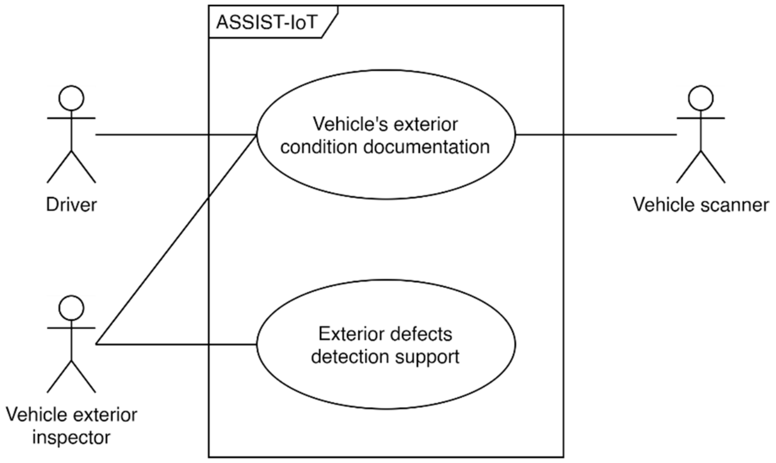
ASSIST-IoT
Vehicle's exterior condition documentation
Driver
Vehicle scanner
Exterior defects detection support
Vehicle exterior inspector

Figure 5.6.1.9-3: Illustration of vehicle exterior condition inspection and documentation

See also oneM2M TR-0026 [i.10], clause 6.1.

5.6.1.10 Use case analysis

IoT Data that may compromise data usability:

- M2M device data provided to Vehicle Service Centre; diagnostics data provided to Vehicle Detection M2M Application. For example, sensor measurements describing the vehicles' operation may be taken at very high sampling frequencies.

- Results of the maintenance evaluation which has to be statistically significant, e.g. at a 95 % confidence level.

- Diagnostic & Maintenance Report from Vehicle Resolution M2M application provided to Vehicle Owner: completeness of the vehicle-scanning report, user-friendliness of the defect-identification process, unambiguous identification of the documented vehicle.

The Applications behind the Vehicle Service Centre need to be able to clearly determine which parts need to be replaced. The data usability and easy understanding by humans of M2M device data is necessary (translation to natural language when relevant). In case of AI, data presentation and integrity are important to ensure a valid AI decision.

Vehicle Owner (and the service technician) needs to understand how urgent is the maintenance, what needs to be replaced and which part needs to be changed. For example, when receiving information about vehicle light, it should know what action needs to be performed and on which side on the vehicle it should be done. If the data is misleading (e.g. only mentioning "defective front light" or indicating a hexadecimal code that leads to another part because the system was improperly setup), the technician may not be able to successfully perform the relevant maintenance. The mechanics (technician) needs also to 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 sensors) and to reset the condition that led to maintenance when it has been fixed. If the report is ambiguous, the mechanics may also order the wrong part.

The consequences of failing this use case because the data were unusable may be very important: safety is not fulfilled in the vehicle and it may lead to accident with potential loss of human lives.

5.6.2 Use Case F.2: Smart Parking

5.6.2.1 Description

Smart parking helps address one of the biggest problems of driving in urban areas: finding empty parking spaces and controlling illegal parking. Parking spaces are wide spread and may be owned by different providers (e.g. mall parking provider and street parking provider) so that it is not easy to access the information at one place/time.

With smart parking service, drivers can easily find available parking spaces, pay parking fees and can even make reservations. Making parking reservations would be available even dynamically for limited people such as VIPs or the disabled, since ordinary parking service needs to satisfy first-come-first-served rule.

In this use case, a user arrives at a mall, but its parking is full. The mall parking provider takes the tentative reservation and moves it to a street parking reservation. Information about the location in the street where to park as well as a discount coupon to compensate the higher parking rate in the street are given to the car driver. This location is close to a location reserved for disabled people. Law enforcement authorities are also included as an actor to prevent parking on reserved spots.

5.6.2.2 Source

oneM2M TR-0026 [i.10], use case in clause 6.13.

5.6.2.3 Actors

- ***[Machine]:*** M2M Service Platform: platform that interacts with M2M gateways/devices and M2M application service providers.
- ***[Device]:*** Smartphone: M2M device which acts as a car navigator and a wallet to pay parking fee by connecting parking meters.
- ***[Device]:*** On-street parking meter: M2M device installed near parking slots to charge drivers parking fees.
- ***[Device]:*** In-building parking sensor: M2M device with a small camera that can recognize a plate on cars, and is installed near disabled-only parking spaces.
- ***[Human]:*** Parking provider: M2M application service provider who owns parking lots. In this use case there are two parking providers: in the mall and on street.
- ***[Human]:*** Billing provider: M2M application service provider (e.g. financial institution) who provides billing service for M2M users, e.g. for parking fees. When bills are issued by M2M application service providers, coupons may be used for compensation schemes. This can also apply for fines issued by police centres.
- ***[Human]:*** Police centre: law enforcement authority, one of M2M application service providers, who charges fine to whom break laws.
- ***[Human]:*** Vehicle driver: M2M service user who drives a car. In the second sub case, dedicated parking space, there are two users. One originally makes a reservation who is handicapped, and the other who illegally parks a car on disabled-only parking area.

- **Data user/consumer:** Parking provider, billing provider, police centre for fining and vehicle driver.

5.6.2.4 Pre-conditions

See oneM2M TR-0026 [i.10],clause 6.13.

5.6.2.5 Triggers

See oneM2M TR-0026 [i.10], clause 6.13.

5.6.2.6 Normal flow

See oneM2M TR-0026 [i.10], clause 6.13.

5.6.2.7 Alternative flow

See oneM2M TR-0026 [i.10], clause 6.13.

5.6.2.8 Post-conditions

See oneM2M TR-0026 [i.10], clause 6.13.

5.6.2.9 High Level Illustration

See oneM2M TR-0026 [i.10], clause 6.13.

5.6.2.10 Use case analysis

IoT data that may compromise data usability:

- Status of parking lot, location of reserved parking area in the street, parking area cost and discount coupon, status of parking area (e.g. disabled-only) in the street and in the mall, vehicle plate information.

As an example, if the vehicle driver is provided with ambiguous or wrong information about available parking area information, he may park on a dynamically allocated disabled-only area or already reserved area and get fined. This may result from the wrong configuration of the service in case parking spots numbers in the IoT system do not match the actual parking spot locations.

The use case also includes a sensor that reports illegal parking to police centre. The provided data should be accurate and delivered in a human-usable format to the policemen.

The consequences of failing this use case because the data were unusable or ambiguous are moderate: a disabled person may not be able to park and go to the mall, the owner of another vehicle may be unduly fined. This is more about a bad quality service level.

5.6.3 Use Case F.3: Port automation: Tracking assets in terminal yard

5.6.3.1 Description

This use case has been contributed by the ASSIST-IoT project. This project aims at designing, implementing, and validating an open, decentralized, reference Next Generation IoT (NG-IoT) architecture, with its corresponding enablers, services, and tools for assisting human-centric applications within multiple verticals. ASSIST-IoT use cases address:

i) port automation;

ii) smart safety of workers; and

iii) cohesive vehicle monitoring and diagnostics.

The ASSIST-IoT system is noted below as the IoT system.

In a port, containers are managed by heavy machinery equipment like Rubber Tired Gantry cranes (RTGs), Rail Mounted Gantry cranes (RMGs), or Ship-To-Shore cranes (STSs). However, they always require the intervention of on-board operators and on-site clerks, who interact with each other by various means and signals, including information sources required to handle and deliver freight. The use case shows how IoT technologies can transform complex industrial processes, infrastructure and equipment managed in the maritime industry.

In the present use case, the main problem to solve is to enable traceability of containers within the port to avoid losing them, and to enhance the operational efficiency of terminal operators (including internal and external drivers). To achieve this, the positions of all Container Handling Equipment (CHE) within the yard, including as well external trucks, needs to be tracked. Additionally, CHEs, using Position Detection System (PDS) or other external positioning system, report all container handling operations, such as picking up and placing down a container by an RTG, or being loaded or unloaded by a Terminal Tractor (TT). The containers being handled need to be identified by CHEs, either automatically or manually by the driver. All this information is combined in the port Terminal Operating System (TOS) in order to track the location of all containers and CHEs within the yard.

The IoT system allows to gain better insight into the operational status of the port, monitoring the situation in real-time, and limiting idling periods. It improves container traceability and minimizes the number of containers lost. Finally, it creates a robust/secure/private system for tracking assets and reusing that information on the edge.

This use case is divided into several sub-use cases:

- Sub use case 1 - Asset location management: All assets (CHEs and containers) within the terminal yard are continuously tracked. The information can be made available to authorized actors.
- Sub use case 2 - CHE location tracking: The location of all container handling equipment (CHE) within the port is always known.
- Sub use case 3 - Container handling operations reporting: CHE carrying out a work order reports every container being handled to the system, including the type of action performed.

5.6.3.2 Source

"Use Cases Manual & Requirements and Business Analysis - Initial", Assist-IoT project report [i.22].

5.6.3.3 Actors

- ***[Human]:*** Terminal management: they are able to monitor the position of all CHEs and containers in the yard using the TOS and PDS. They can also retrieve historical data collection.
- ***[Human]:*** Container Handling Equipment (CHE) drivers. They use an application that aids in reporting operations. For external truck drivers, this application is installed on a mobile device; internal CHE drivers have a mounted device in their cabin.
  - internal drivers run the app on the mounted device.
  - external drivers have received a mobile device with a temporary identity.
- ***[Machine]:*** Terminal Operating System (TOS)
- ***[Devices]:*** CHEs, CHE Position Detection System (PDS)
- **Data user/consumer:** Terminal management staff; Terminal Operating System (TOS).

5.6.3.4 Pre-conditions

Terminal Operating System (TOS), Container Identification System, Device with Temporary ID (for External drivers), Frontend adapted to mobile screens.

Sub use case 1: CHEs are equipped with devices for reporting their operational status.

Sub use case 2: CHE is within a defined operational area.

Sub use case 3: CHE is carrying out a work order.

5.6.3.5 Triggers

Sub use case 1: None.

Sub use case 2: CHE is turned on.

Sub use case 3: CHE handles a container.

5.6.3.6 Normal flow

Sub use case 1:

1) CHEs report their location and container handling operations to the IoT system.
2) The IoT system aggregates and buffers the retrieved information.
3) The IoT system forwards the information to the TOS for real-time tracking and historical data collection.
4) The IoT system exposes the information to other actors with sufficient authorization.

Sub use case 2:

1) CHE attempts to determine its location using GPS.
2) CHE retrieves its absolute location from GPS.
3) CHE reports its coordinates to the IoT system.

Sub use case 3:

1) CHE is to handle a container.
2) CHE identifies the container.
3) CHE reports to the IoT system the operation being performed, and the container being handled.
4) CHE proceeds with its work order.
5) CHE reports to the IoT system that the container movement operation has been successfully performed.

5.6.3.7 Alternative flow

Sub use case 2:

CHE is unable to retrieve its absolute location, or the measurement precision is too low.

1) CHE determines its relative location using nearby beacons and/or machines.
2) CHE reports its relative location to the IoT system.
3) The IoT system translates the relative location into absolute coordinates.

5.6.3.8 Post-conditions

Sub use case 1: End-user is presented with information about assigned asset's location in a given moment.

Sub use case 2: End-user is presented with information about assigned asset's location in a given moment.

Sub use case 3: All CHEs report every related movement of containers.

5.6.3.9 High Level Illustration

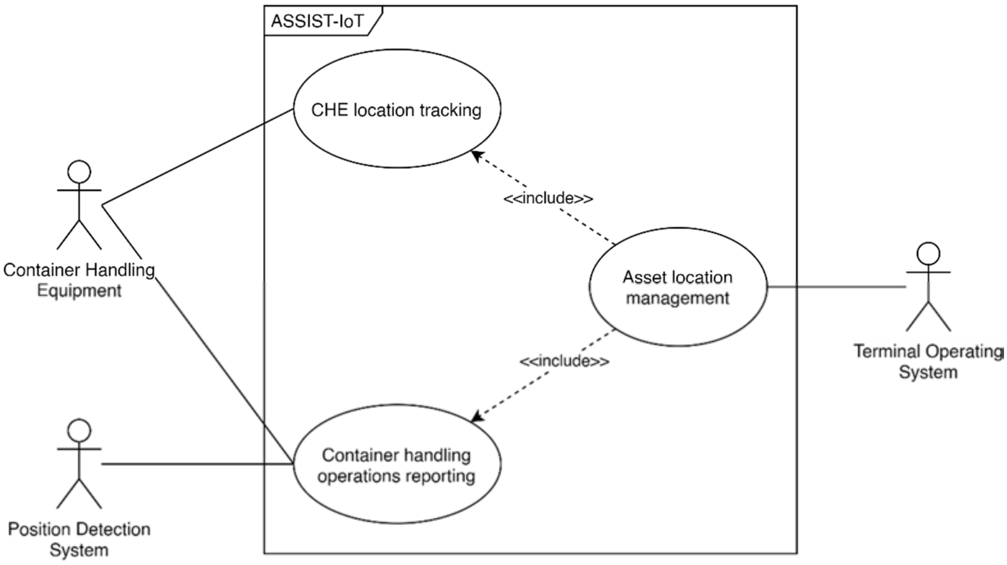
ASSIST-IoT
CHE location tracking
<<include>>
Asset location management
<<include>>
Container handling operations reporting
Container Handling Equipment
Position Detection System
Terminal Operating System

Figure 5.6.3.9-1: Illustration of port automation system

5.6.3.10 Use case analysis

Data that may compromise data usability:

- Identification and location of CHEs and containers in the terminal yard.
- Identification of other devices within the terminal yard.
- Information about operation on containers handled by CHEs.
- Route recording of every CHE with time and position of communication.
- Timestamp and location of where the container is picked up and placed.

Container identification:

- Some RTGs can be equipped with an external container identification system based on OCR (reading container ID).
- Otherwise, the container has to be identified manually by the driver.
- In some cases (e.g. for truck drivers) the identification will be impossible to perform. Then, The IoT system has to assume the container being handled is the one that was specified in the work order.

Location management should be done in a scalable manner as many objects need to be tracked reliably with position, identification and timestamp.

Data from all objects should be synchronized (e.g. identical time reference).

Objects' position should be of sufficient precision. In this use case, the IoT system is constantly aware of the position of every CHE with an accuracy of ±0,5 m.

The identification of each object (CHE, container, other devices in the terminal yard) should be unique to prevent invalid information and mishandling of containers.

Lack of usability of the data in this use case may result in the loss of containers, which has mainly economic consequences.

5.6.4 Use Case F.4: Port automation: RTG remote control with Augmented Reality (AR) support

5.6.4.1 Description

This use case has been contributed by the ASSIST-IoT project [i.22]. It is in an extension to Use Case F.3, Sub Use Case 3.

In a traditional container terminal layout, the yard cranes can be manned- Rubber-Tired Gantry cranes (RTGs) or manned-Rail Mounted Gantry cranes (RMGs). They can be working in a typical two crane per-stack configuration with various possibilities: end-feed-RMG, side-feed-RMG and RTG. The productivity per crane naturally depends upon the skills and attitude of the crane driver, and many other factors related to the processes involved in the terminal.

Furthermore, when one looks at a fleet of manned-yard cranes, they are dispersed across the container's stacks. The overall logistics is even more complicated, taking into account transporting the operators to and from the cranes, climbing into the cabins, toilet breaks, lunch breaks, and so on. Finally, supervision across the container stacks can be challenging at times, and communication could be complicated between the supervisors and the crane operators, and between crane operators themselves.

Remote operation enables the control of several cranes by one driver who can virtually jump from one location to another. This allows to optimize the efficiency of the driver to a completely different level. The idling time can be reduced from 60 % up to 25 %.

The use case can be implemented at two functional levels:

- Sub use case 1: The operators control the RTG wirelessly using a console with built-in enhanced visuals to aid them in performing the work order.
- Sub use case 2: The remote RTG operator is provided with Augmented Reality (AR) guide of which container to pick up and where to place it.

5.6.4.2 Source

"Use Cases Manual & Requirements and Business Analysis - Initial", Assist-IoT project report [i.22].

5.6.4.3 Actors

- ***[Human]:*** Terminal management: they are able to monitor the position of all CHEs and containers in the yard using the TOS and PDS. They can also retrieve historical data collection.
- ***[Human]:*** Remote RTG operator.
- ***[Machine]:*** Terminal Operating System (TOS)
- ***[Devices]:*** RTGs, containers
- **Data user/consumer:** Terminal management staff, Remote RTG operator; Terminal Operating System (TOS).

5.6.4.4 Pre-conditions

- The operator is set to execute a work order.
- The RTG is ready for remote operation.
- There is a stable wireless network connection between the operator and the RTG.
- The operator is executing a work order remotely.

5.6.4.5 Triggers

The operator starts executing the work order.

5.6.4.6 Normal flow

Sub use case 1:

1) The operator receives work orders on their terminal.
2) The operator selects the work order to perform from their terminal.
3) The operator selects the RTG to be controlled.
4) The operator starts carrying out the assigned work order.
5) The IoT system provides a network connection between the operator and the RTG.
6) The operator finishes the work order.
7) The operator is ready to select the next work order.

Sub use case 2:

1) The operator starts performing a work order.
2) The IoT system obtains the information about the work order from the TOS.
3) The IoT system is aware of the position of the RTG and the location of the container in the yard is obtained (UC F.3).
4) The IoT system guides the operator to the container.
5) The RTG camera system provides the video feed from the RTG.
6) The IoT system identifies the container to be picked up in the video feed, based on the previously retrieved information.
7) The IoT system provides AR support to the operator by highlighting the container to be picked up on the RTG video stream from the RTG camera system.
8) The operator orders the RTG to pick up the container.
9) The IoT system guides the operator to the target yard slot.
10) The IoT system identifies the target slot in the video feed.
11) The IoT system provides the operator with AR video feed from the RTG camera system. The target slot is highlighted.
12) The operator orders the RTG to place the container.

5.6.4.7 Alternative flow

N/A.

5.6.4.8 Post-conditions

Sub use case 1: The RTG idling time is reduced from 60 % up to 25 % (35 % savings).

Sub use case 2: The object (i.e. container) detection mean average precision is larger than 75 %.

5.6.4.9 High Level Illustration

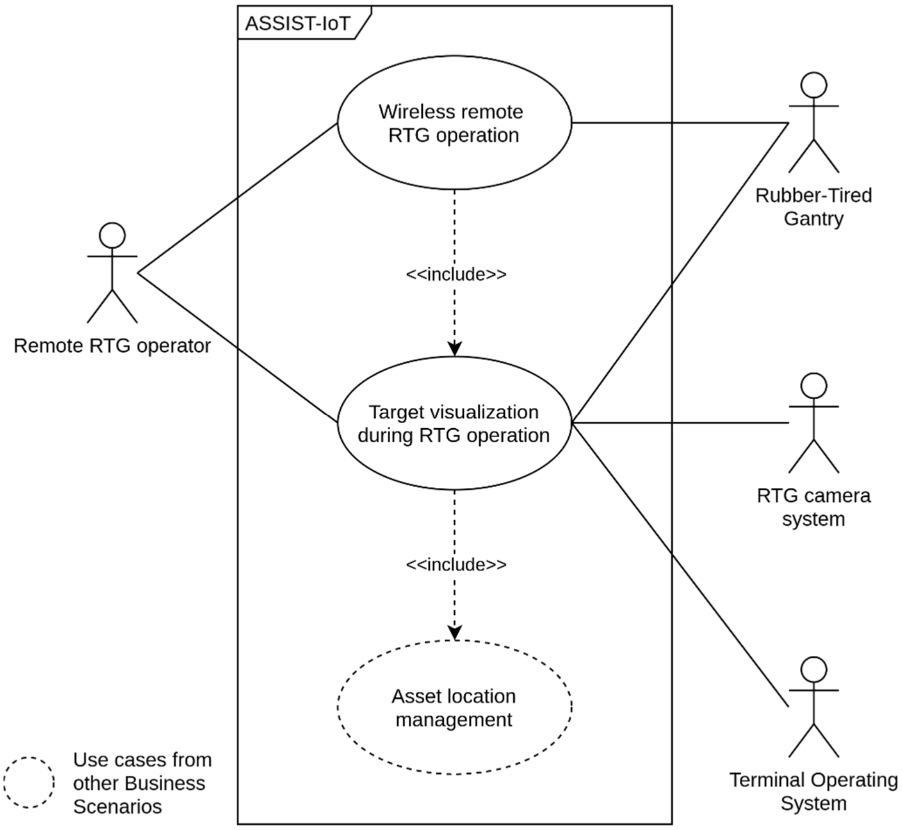
ASSIST-IoT
Wireless remote RTG operation
<<include>>
Target visualization during RTG operation
<<include>>
Asset location management
Remote RTG operator
Rubber-Tired Gantry
RTG camera system
Terminal Operating System
Use cases from other Business Scenarios

Figure 5.6.4.9-1: Illustration of RTG remote control with Augmented Reality (AR) support

5.6.4.10 Use case analysis

Data that may compromise data usability:

Video feed from RTG camera system, information about the location of containers within the terminal yard, TOS work orders, data from and commands for moving crane parts (hoist, gantry, straddle).

Data from all objects should be synchronized (e.g. identical time reference).

Objects' position should be of sufficient precision.

Video feed from RTG camera system should be real-time with low latency.

Work orders should be understandable by the TOS.

Reporting from actions performed by the RTG should be reliable.

Lack of usability of the data in this use case may result in the loss of containers, which has mainly economic consequences. However, it may also have stronger consequences, but with very low probability, as a mishandled container may create an accident on the terminal yard with potential lives lost.

5.6.5 Use Case F.5: Autonomous driving

5.6.5.1 Description

Autonomous Driving (AD) refers to the capability of the vehicle to drive from one location to another, without intervention from humans, and in a safe way, without incurring damage to surroundings (pedestrians, buildings, other vehicles) and to its (vehicle) passengers.

In autonomous driving, it is essential for the vehicle to have a complete awareness of its own state and of the state of its surroundings. In that respect, data that is lost, ambiguous, invalid or which arrives with large delay, introduces uncertainty in the vehicle's dynamic model of its environment. This uncertainty will typically result in vehicle taking appropriate measures to deal with it, typically decreasing the speed of the vehicle, or stopping it altogether. Reasoning behind this is that for safety critical applications, safety is in the first place. Modern vehicles are equipped with a large number of sensors which are increasing comfort, fuel efficiency and safety of vehicles. This wide variety of sensors measures and collects data about the vehicle itself (for example: ABS sensors, brake switch, speed, location, etc.), but also observe the state of the vehicle's environment - using radar, camera, short range distance measurement sensors, LIDAR, etc.

Furthermore, the roads and surrounding infrastructure are also becoming more instrumented with sensors and able to communicate. The possibility of interconnecting infrastructure sensors (cameras, traffic light radars, road sensors, etc.) and thus exchanging data with vehicles may lead to new ways to design autonomous vehicle systems, thereby reducing cost, while increasing robustness and reliability of autonomous driving.

Other connected objects (pedestrian's smartphones, for example) may also act as additional sources of data for autonomous driving vehicle, thereby contributing to improved efficiency, accuracy and safety of the autonomous driving functions.

Systems supporting the combination of all these data sources will enable pushing the driving automation to the higher levels of automation, ultimately to one where the driver is out of the (control/driving) loop. Therefore, by making autonomous cars an IoT entity, this will enable larger groups of developers to create IoT/AD services.

5.6.5.2 Source

This use case has been adapted from oneM2M TR-0026 [i.10], use case in clause 6.18.

5.6.5.3 Actors

- ***[Device]:*** IoT Device: IoT devices are embedded in vehicles, roads and associated infrastructure, as well as in devices used by other participants in traffic (pedestrians, cyclists). Each IoT device collects and sends data to IoT platform, and can receive data from IoT platform.
- ***[Human]:*** Vehicle Driver: Driver sits in its normal (driving) position, and is in position to take corrective action (level 3, level 4) when prompted to do so by the autonomous driving system. There is no vehicle driver at level 5 of automation.
- ***[Machine]:*** IoT platform provider: It operates an IoT platform which is collecting data from vehicles, other participants in traffic (pedestrians, cyclists), from roads and associated infrastructure (traffic lights, cameras, etc.).
- ***[Machine]:*** Autonomous driving application (ADApp) provider: Party that is providing the ADApp which may run on local or remote AS (Application Servers). Remote AS connects to the IoT platform, and from there it collects relevant data needed to run an ADApp - for example LDM (Local Dynamic Map).
- **Data user/consumer:** IoT platform, Vehicle Driver, Autonomous driving application

5.6.5.4 Pre-conditions

See oneM2M TR-0026 [i.10], clause 6.18.

5.6.5.5 Triggers

See oneM2M TR-0026 [i.10], clause 6.18.

5.6.5.6 Normal flow

See oneM2M TR-0026 [i.10], clause 6.18.

5.6.5.7 Alternative flow

See oneM2M TR-0026 [i.10], clause 6.18.

5.6.5.8 Post-conditions

See oneM2M TR-0026 [i.10], clause 6.18.

5.6.5.9 High Level Illustration

See oneM2M TR-0026 [i.10], clause 6.18.

5.6.5.10 Use case analysis

IoT data that may compromise data usability:

- Sensor data, geolocation, instructions to driver or to actuators.

These data may become unusable in many manners:

There are low chances that sensors are improperly setup in the vehicle, but this may happen in the surrounding of the vehicle. But even the data generated by the vehicle sensor may become unusable if a sensor becomes defective. Checking and maintaining the IoT system in the vehicle is thus if primary importance. Applying lower confidence to data captured from the environment may be important as well.

As in all mobility use cases, the objects position should be of sufficient precision to ensure valid decision making by the AI process and the ADApp.

Ambiguous instructions to drivers and/or actuators, or failing to prompt the driver in a correct manner may result in both vehicle and driver wrongly relying on each other to cope with a safety issue.

Finally, the AI process receives data from a very large number of sources. They should be clearly presented and if possible aggregated across the system to enable a smooth running of the AI process.

Lack of usability of the data or compromised data in this use case may result in the lack of sufficient safety at the vehicle level, potential accident (e.g. the example of camera blinded by the brightness of the sun light which caused an accident by an autonomous car). This may result in some cases in the potential loss of human lives.

5.7 Energy Use Case

5.7.1 Use Case G.1: Energy optimization using AI

5.7.1.1 Description

With the trend of Network Function Virtualisation (NFV), more and more DCs will be deployed to replace the traditional Central Offices in the operators' network. The data centres (DC) are made up of many servers with huge power consumption. Typically, the servers in a DC take 70 % of the total power consumption. The other equipment including switches, routers, storage equipment and air conditioners take the other 30 % of the total power consumption. The servers are deployed and running to meet the requirement of peak hour service, which means the servers are normally at high power-up state at full time even in non-peak hours.

It is possible to move the services to some of the servers and turn the other servers to idle or underclocking state in non-peak hours, with the aim of optimizing the power usage at the DC. It should be noted that such mechanism of energy optimization can be applied widely to other network resources in addition to data centres.

This use case elaborates on how NFV and AI can be combined to optimize usage of the energy in networks and to also show the consequence if there is no good data usability.

5.7.1.2 Source

Derived from ETSI GR ENI 001 [i.6].

5.7.1.3 Actors and Roles

- ***[Human]:*** Operator: manages the DCs and confirms the VM/Container migration policies and scale in/out policies.
- ***[Machine]:*** ENI System: collects and learns service pattern from the data collected from the DC servers which houses the sensors; determines the VM migration policies and scale in/out policies according to prediction of the service requirements; triggers steering of the service flows from one VM to another VM.
- ***[Machine]:*** DC servers: provide the required information to the ENI system, execute the VM migration and VNF scale in/out according to the policies.
- ***[Machine]:*** DC environmental monitoring and control system: provide the required information to the ENI system, and execute the operation of environmental adjustment.
- ***[Machine]:*** NFV MANO: executes the lifecycle management operation of the VNFs according to policies.
- **Data user/consumer:** ENI System.

5.7.1.4 Pre-Condition

All servers in the DC are running all time and the energy consumption is high. The ENI system performs some initial actions related to the collection of information, use of AI algorithms and service patterns learning.

5.7.1.5 Triggering conditions

The following trigger types associated with the ENI system may be identified:

- The ENI system predicts that the required resources of a service will fall below a certain threshold in a certain period.
- The ENI system predicts that the required resources of a service will grow up higher than a certain threshold in a certain period.
- The ENI system decides to change the DC environmental settings.
- The ENI system detects a change of the service pattern learned before.

5.7.1.6 Normal Flow

The following initial sequence of actions may be identified:

1) The ENI system collects and stores information of the virtual networks, including CPU usage, storage usage, and network usage for each VNF, etc., as well as the power consumption information and environmental information.

2) The ENI system uses AI algorithm to build the relations between the network service and its required resources, and the relations between the power consumption and the environment settings including e.g. the location of the running servers, the setting of the cooling system, etc.

3) The ENI system learns the service pattern and predicts the required resources of the service in a certain period in the future, e.g. the next hour.

5.7.1.7 Alternative Flow

1) When the ENI system predicts that the required resources of a service will fall below a certain threshold in a certain period, and the service configured by the operator as able to be moved, the ENI system triggers, directly or indirectly, the NFV MANO system to migrate the services and VMs/Containers providing this service to another selected server:

   a) If the VMs/Containers on one server are all migrated to another server, the spare server is turned into idle mode.

2) When the ENI system predicts that the required resources of a service will grow up higher than a certain threshold in a certain period, the ENI system triggers the scale out of the existing VNF and bring up new VMs/Containers:

   a) If the running servers cannot provide the required resources of a new VM/Container according to prediction, the ENI system wakes up a selected idle mode server.

3) The ENI system may decide to change the DC environmental monitoring and control system to adjust the environmental settings when a server is woken up or turned into the idle mode.

4) When the ENI system detects a change of the service pattern learned before, the ENI system will adjust the VM/Container migration policies and scale in/out policies.

5.7.1.8 Post-conditions

Servers in the DC are dynamically turned to idle and waken up according to the service pattern; therefore, the cost of power consumption is reduced as much as possible, see clause 5.2.3.2.7 in ETSI GS ENI 001 [i.6].

5.7.1.9 High Level Illustration

See clause 5.2.3.3.3, Figure 5.4: Procedure for energy optimization using AI in ETSI GS ENI 001 [i.6].

5.7.1.10 Use case analysis

Data that may compromise data usability: data received from the virtual networks.

The data within ENI system is received from software sensors, however if the data is compromised as a result of corrupted sensor interface, the data is no longer usable by the machine or it could also mean that the machine process the wrong data to give false instruction indicating the power does not to be switched to save power. Although this may not in itself be life threatening but it could mean the DC is not operating at its optimized level. The worst-case scenario could mean that a particular server is over used and may cause system to shut down and make service unavailable.

Comment: The data are from software sensors but they still apply here when it comes to data usability.

5.8 Building Use Case

5.8.1 Use Case H.1: Predictive Operations: Cleaning and waste removal notification service and warning

5.8.1.1 Description

The use case provides cleaning staff with data on room usage and notifications when a room needs cleaning. The goal is to enable the cleaning and waste removal team to:

- Reduce the time needed to check rooms.
- Sort areas hierarchically according to their projected needs.
- Redirect personnel to abate critical situations.
- Update and revise their schedules based on statistical use of the rooms.

This will enable them to save time, and to target their efforts to offer a better or equally good service at a lower cost.

The Value-Added Service will process data from non-intrusive sensors mounted in rooms and toilets. The data is not linked to personal information on who has entered the room. The sensors register if a person passes the door (in an anonymized way), and can thus keep track of the approximate number of people who have visited.

5.8.1.2 Source

VICINITY_D5_2_VICINITY_valueadded_services_implementation_framework_1.0.pdf [i.14].

5.8.1.3 Actors

- ***[Human]:*** Building managers.
- ***[Human]:*** Tenants.
- ***[Human]:*** Cleaning and waste removal team.
- **Data user/consumer:** Building Manager.

5.8.1.4 Pre-conditions

N/A.

5.8.1.5 Triggers

N/A.

5.8.1.6 Normal flow

Cleaning and waste removal notification service and warning clause 2.1.1.1, part of use case 1a.1 - Predictive operations, [i.14].

5.8.1.7 Alternative flow

N/A.

5.8.1.8 Post-conditions

Individual and statistical analysis of rooms clause 2.1.2.2, part of use case 1a.1 - Predictive operations, [i.14].

5.8.1.9 High Level Illustration

Figure 2-1 Use Case 1a.1 - Overview in clause 2.1.1.1, part of use case 1a.1 - Predictive operations, [i.14].

5.8.1.10 Use case analysis

Data that may compromise data usability: Data collected by sensor to indicate amount of time room was visited, e.g. door sensor, number of steps movement inside a building could be wrong if sensor is faulty.

These data can be sent to machine to analyse the threshold limit may mean that the rooms are not cleaned for the next users or the cleaners are called to clean when it is not needed and this will result in charging the business for work not needed.

5.8.2 Use Case H.2: Building automation - Environmental monitoring

5.8.2.1 Description

In this use case, several sensors are installed in a building and each sensor performs measurements following a pre-defined measurement interval. The measurement data might include temperature gauge, smoke detector. A Local Controller collects the measurement data from its sensors and may transmit it to the Building Management System at a certain interval. This will allow adjustment to be made to the building temperature or to detect smoke and send set off the water spray for example. It is important that the transmission is reliable and all sensor values are collected within the measurement interval.

5.8.2.2 Source

Study on Communication for Automation in Vertical domains (CAV): 3GPP TR 22.804, clause 5.2 [i.15].

5.8.2.3 Actors

- ***[Human]:*** Building managers.
- ***[Device]:*** Sensors.
- **Data consumer:** Building Managers.

5.8.2.4 Pre-conditions

There are several Local Controllers installed in the building, each connected with many sensors.

5.8.2.5 Triggers

None.

5.8.2.6 Normal flow

At the measurement interval, and with the needed sampling, the Local Controller sends a request to all its sensors in the building to report their measurements.

5.8.2.7 Alternative flow

None.

5.8.2.8 Post-conditions

Every sensor reports their measurements and measurements are received with 99,999 % reliability. The Local Controller collects these measurements and may transmit them to the building management System.

5.8.2.9 High Level Illustration

None.

5.8.2.10 Use case analysis

Data that may compromise data usability: Data collected by sensors to indicate the energy levels in rooms.

If these data are false due to faulty sensor or wrong interval of measurement of sensors, as an example, during setup. This may indicate that the wrong temperature is computed and this may lead to wrong adjustment of the temperature in the building. This consequently may lead to false alarm being raised.

5.8.3 Use Case H.3: Building automation - Home Energy Management

5.8.3.1 Description

This use case is to manage energy consumption at home so that consumers can be aware of their daily home energy consumptions and able to control this consumption by remote actions on home appliances. Innovative services can be developed from the data (energy) collection and sent to either the consumers/ equipment or to Business-to-Business market. The use case focuses on a home Energy GateWay (EGW) that collects energy information from the electrical home network and communicates it to an M2M system for aggregating and processing of the data. Services can then be developed from the collected data.

The EGW performs an initial treatment of the data received from various sources (sensors, context) as follows:

- Aggregating and processing the obtained information.
- Sending some information to the remote M2M system e.g. sending alerts through the M2M system.

- Using some information locally for immediate activation of some actuators/appliances.
- Is connected (wirelessly or via wireline) to home devices, including the home electrical meter, for information on global or individual consumption of the appliances.
- Providing displayable consumed energy-related information to the end-user/consumer terminals (PC, mobile phone, tablet, TV screen, etc.).

5.8.3.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5].

5.8.3.3 Actors

- ***[Human]:*** Home User: user of home appliance.
- ***[Human]:*** Communication operators: in charge of communicating the collected information via any protocol.
- ***[Machine]:*** Energy gateway SP: in charge of collecting & transmitting securely energy information from appliances to the M2M system and receiving remote controls/commands from the M2M system.
- ***[Machine]:*** System operators/providers of service layer platform(s): in charge of providing services/common functionalities for applications (e.g. HEM) that are independent of the underlying network(s).
- ***[Machine]:*** Application Service Provider: Provides Home Energy Management (HEM) Application for the user through the M2M system.
- **Data consumer:** Home User.

5.8.3.4 Pre-conditions

There are sensors installed and connected in the building.

5.8.3.5 Triggers

N/A.

5.8.3.6 Normal flow

See oneM2M TR-0001-Use_Cases_Collection [i.5], clause 9.

5.8.3.7 Alternative flow

See oneM2M TR-0001-Use_Cases_Collection [i.5], clause 9.

5.8.3.8 Post-Conditions

See oneM2M TR-0001-Use_Cases_Collection [i.5], clause 9.

5.8.3.9 High Level Illustration

See oneM2M TR-0001-Use_Cases_Collection [i.5], clause 9.

5.8.3.10 Use case analysis

Data that may compromise data usability: Data collected by sensors to indicate the energy levels in rooms.

These data if false may indicate that the wrong information is submitted to the EGW and leads to false adjustment of appliance which could be harmful and unsafe, another scenario is if the appliance does break, it can become expensive especially if this happens on a frequent basis.

5.8.4 Use Case H.4: Smart safety of workers at building construction site

5.8.4.1 Description

This use case has been contributed by the ASSIST-IoT project in their deliverable [i.22] (also see clause 5.6.3 for more information on the ASSIST-IoT project).

Within any building construction site, a large number of people with various levels of training and experience, are occupied by several subcontracted companies, interact with each other, operate equipment or interface with heavy machinery. Collecting reliable and relevant information in order to generate intelligent insights for the protection of all individuals present at any worksite within a large construction site is one of the aims of this use case. The main objective of this application is the prevention and near real-time detection of common OSH hazards such as stress, fatigue, overexposure to heat and UV radiation, slips, trips, falls from height, suspension trauma, immobility due to unconsciousness, collision (forceful impact) with heavy equipment, entrapment (unable to evacuate the worksite during an emergency) and improper use of PPE.

The physiological parameters of the construction workers are being monitored in real-time using wearable sensors in order to ensure that their health and safety is protected at all times while at the construction site. Mobile processing units are used to locally assess the worker's fatigue and stress level, without transmitting sensitive information to a central location unless a serious incident occurs.

The construction workers' location within the construction site is monitored so that first responders can be sent in case of an emergency. Geofencing services are also supported to ensure that construction workers move around areas within which they are authorized and trained to be.

Construction workers and the project's OSH manager are provided with relevant information about incidents and potential hazards. The OSH manager combines, only a relevant subset of, real-time data with information that are manually provided from the entire workforce via existing management and collaboration platforms in order to assess and report the overall risk status for the construction site.

When a construction worker requests navigation instructions from his current location to a worksite, he should follow approved walking paths through areas the worker is authorized to access. In case of an emergency the workers receive evacuation instructions along predefined routes. The emergency routes are updated by the OSH manager according to the evolving situation based on the routes followed by safely evacuated workers. All paths and routes should be indicated on the BIM.

This use case is divided into several sub-use cases:

- Sub use case 1 - Occupation safety and health monitoring - Workers' health and safety assurance: Monitor and protect the construction workers' personal health and safety. Notify the OSH manager about incidents or undesirable behaviour in the construction site.
- Sub use case 2 - Occupation safety and health monitoring - Geofencing boundaries enforcement: Enforce area-based access restrictions within the construction site.
- Sub use case 3 - Safe navigation instructions: Provide a safe route to the worker through the construction site.

5.8.4.2 Source

"Use Cases Manual & Requirements and Business Analysis - Initial", Assist-IoT project report [i.22].

5.8.4.3 Actors

- ***[Devices]:*** Real-time wearable sensors and actuators (e.g. thermometer, cooling system etc.), weather station, PPE tags. Sensitive information is transmitted to a central database only in case of an identified incident or as a frequent status report summary.
- ***[Machine]:*** Building Information Modelling (BIM) system: system of software systems and services that are used for hosting and authoring the digital description of every aspect of the built asset. It contains OSH and quality assurance information which is used to manage and communicate with companies that are subcontracted to work on the project on behalf of the main contractor.

- ***[Human]:*** Construction worker: persons occupied at a building construction project. Employees who are subcontracted by the main contractor are also included. They use real-time wearable sensors while at the construction site. The construction worker is provided with an interface to send a notification in case of an emergency.

- ***[Human]:*** OSH manager: manager responsible for overseeing compliance to OSH regulations and for managing the related risks at the construction site.

- ***[Human]:*** Construction plant operator: he operates the construction plant. He is employed by companies that are subcontracted by the main contractor that manages the project and the construction site.

- **Data user/consumer:** OSH manager; BIM system.

5.8.4.4 Pre-conditions

All the construction workers wear their personal protective equipment and smart wearables. A construction worker may be operating construction plant or working at height. All access points are securely locked and the construction workers and plant have been registered with the main contractor. Smart devices and wearables are paired together in order to monitor the construction worker's status, e.g. wearing all PPE or operating construction plant.

Sub use case 1: The construction worker is at the construction site wearing their Personal Protective Equipment.

Sub use case 2: Restricted areas are defined in the system (GPS coordinate of Construction plants, dangerous area, within the BIM System) by the OSH manager.

Sub use case 3: The BIM includes:

- as-is information about the construction site;

- approved walking paths;

- approved emergency evacuation paths;

- emergency assembly points.

5.8.4.5 Triggers

Sub use case 1 and sub use case 2: Time-based, continuous monitoring while the construction worker is in the construction site.

Sub use case 3: The construction worker is at the construction site and requests navigation instructions or receives an evacuation alert.

5.8.4.6 Normal flow

Sub use case 1:

1) The IoT system is aware of the construction worker's identity and pairs them with their smart PPE.

2) The IoT system tracks the location of the construction worker. The IoT system is aware of the construction worker's authorization to access specific areas within the construction site.

3) The IoT system verifies that the construction worker is not near a geofenced area (UC-P2-2 and UC-P2-3).

4) The IoT system monitors the weather conditions at the construction site, the exposure of the construction worker to UV radiation, the physiological parameters of the construction worker, and the motion pattern of the construction worker's body.

5) The IoT system analyses all the collected data from all the construction workers who are present at the construction site and identifies no increased risk of exposure to OSH-related hazards for the construction worker.

6) The IoT system analyses the motion patterns of the construction worker in order to verify that they are normal with respect to their assigned activity.

7) The IoT system has not detected any increased risk to the construction workers health and safety, but they notify the OSH manager by raising an alarm through ASSIST-IoT.

Sub use case 2:

1) The IoT system is tracking the location of the construction worker.

2) The IoT system verifies that the construction worker is authorized to be at their current location.

Sub use case 3:

1) The IoT system tracks the location of the construction worker.

2) The construction worker requests from The IoT system navigation instructions to a destination within the construction site.

3) The IoT system is updating information about the as-is state of the construction site and approved walking paths based on information from the Building Information Model.

4) The IoT system provides navigation instructions along approved routes to their mobile device.

5) The construction worker confirms safe arrival at their destination.

5.8.4.7 Alternative flow

Sub use case 1:

1) The IoT system detects increased risk of overexposure to heat.

2) The IoT system actuates the protection from overexposure to heat process.

3) The construction worker is adjusting the overexposure-to-heat protection process and The IoT system records the construction worker's preferences.

4) The IoT system verifies that the risk has been reduced and stops the overexposure-to-heat protection process.

5) The IoT system notifies the OSH manager about the incident.

6) ASSIST detects an increased risk of extreme fatigue or overexposure to UV radiation.

7) The IoT system notifies the construction worker and alerts the OSH manager.

8) The IoT system detects abnormal motion patterns.

9) The IoT system notifies the OSH manager.

Sub use case 2:

1) The IoT system detects that a construction worker is approaching a location at which they are not authorized to be.

2) The IoT system alerts the construction worker and notifies the OSH manager.

Sub use case 3:

1) The IoT system receives an emergency evacuation alert from the OSH manager.

2) The IoT system alerts the construction worker and provides navigation instructions for safe evacuation from their current location based on approved evacuation routes.

3) The IoT system updates the evacuation navigation instructions based on real time information from the evacuation paths followed by all the construction workers.

4) The OSH manager indicates on the Building Information Model hazardous areas that should be avoided by construction workers during the evacuation process.

5) The IoT system updates the evacuation navigation instructions.

6) The construction worker confirms safe arrival at the emergency assembly point.

5.8.4.8 Post-conditions

Sub use case 1:

- The first responders are promptly notified about the occurrence, nature and location of an emergency and rescue the construction worker who is in danger.
- The construction worker can instantly notify the OSH manager in case of an emergency.
- Unauthorised access to restricted worksite zones is prevented.
- The construction site's incident log is updated.

Sub use case 2:

- Construction workers are alerted.
- The OSH manager is notified about any unsafe behaviour or incidents.
- The construction site's incident log is updated.

Sub use case 3:

The construction worker arrives at the worksite or at an emergency assembly point.

5.8.4.9 High Level Illustration

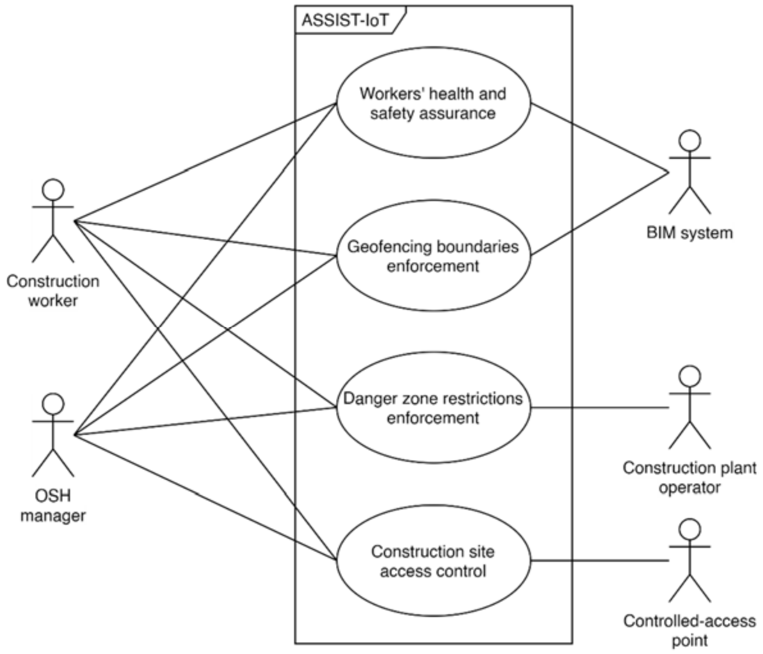
ASSIST-IoT
Workers' health and safety assurance
Geofencing boundaries enforcement
Danger zone restrictions enforcement
Construction site access control
Construction worker
OSH manager
BIM system
Construction plant operator
Controlled-access point

Figure 5.8.4.9-1: Illustration of occupation safety and health monitoring

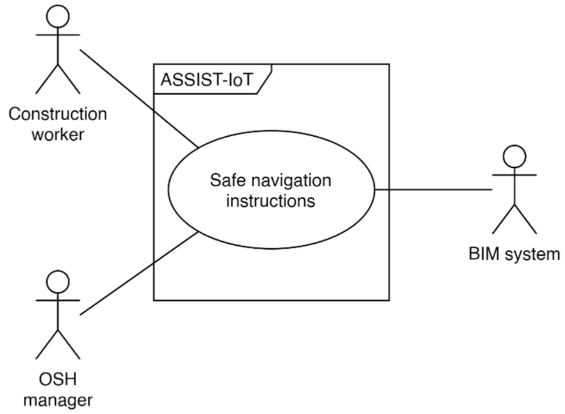

Figure 5.8.4.9-2: Illustration of safe navigation instructions

5.8.4.10 Use case analysis

Data that may compromise data usability:

Location and proximity data of workers on site, physiological parameter measurements, weather conditions measurements, personal identification information, training and medical records, building information, users' thermal comfort preferences, alerts and notifications.

Location data should be of sufficient precision and reported in real-time.

User interface in construction worker's device should be easily understandable, whatever the language and reading level of the worker.

Reporting should be relevant to enable fast decisions as needed by OSH manager.

Data flow from all devices should be secured and respect privacy, as well as guarantee data integrity.

The BIM should be setup without any ambiguity or invalid information, as this may lead to invalid navigation and put the workers at risk. Clarity of navigation instructions based on user feedback.

Lack of usability of the data or compromised data in this use case may result in limited safety for the site workers, which may have strong consequences in case of false negatives (unhealthy conditions are not detected or invalid navigation instructions that drive the worker to a hazardous area). If the consequence is raising false positives, the impact is lower, just leading the worker to be further screened while there is no issue.

5.8.5 Use Case H.5: Machine socialization

5.8.5.1 Description

A robot is designed to clean rooms in hotel. The task of the robot is to keep all rooms clean. If the hotel has only one robot, it has to clean rooms one by one. If the hotel has two robots, they will complete the task more efficiently if they cooperate with each other. If robot A has cleaned a room, it may inform the other robot that this room has been cleaned, so robot B can move to another room for clean job. This implies that if multiple robots share a same task, cooperation will improve the efficiency. As in the hotel scenario, the robots' owner may not tell the robots explicitly that there exists another robot with the same task. So, firstly, the robot should have the capability to discover other robots and find out if they share the same task as itself. Secondly, a robot should realize what kind information will affect other robots' behaviour, and it should transmit messages in order to share this information to other co-operators. For example, after a machine scan a room, it will find out the clean status of that room (clean or dirty), when a robot is cleaning a room or after it is cleaned, it will change the status of that room, the information will affect other robots' behaviour, because for any other robots it is unnecessary to go to a room that is being cleaned or has been cleaned by another robot. Thirdly, a robot should have the knowledge about the message interface of other robots. Only with this knowledge, it can send inform or command to another robots.

A cloud robot service platform may play an important role in this hotel scenario. Because the platform may help robots to discover each other, and the platform may initialize a powerful commander to optimize the job with multiple robots.

5.8.5.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5], clause 6.2.

5.8.5.3 Actors

- ***[Machine]:*** The clean robot is designed to keep all rooms clean. They may cooperate with each other directly or with the help of cloud robot service platform.
- ***[Machine]:*** Cloud robot service platform can discover the underline cooperation between machines.
- **Data user/consumer:** Cloud Robot service platform.

5.8.5.4 Pre-conditions

- Multi-robots share the same tasks or correlated tasks.

5.8.5.5 Triggers

A robot discovers another robot with the same or correlated tasks.

5.8.5.6 Normal Flow

- A robot A is deployed in a hotel.
- Another robot B is deployed in a hotel.
- Robot A and B discover each other (the discovery is performed by themselves or aided by the cloud robot service platform).
- Robot A share information to robot B and Robot B share information to Robot A.
- The cloud robot service platform helps to optimize the task process and help the robots to cooperate with each other.

5.8.5.7 Alternative Flow

None.

5.8.5.8 Post-conditions

N/A.

5.8.5.9 High Level Illustration

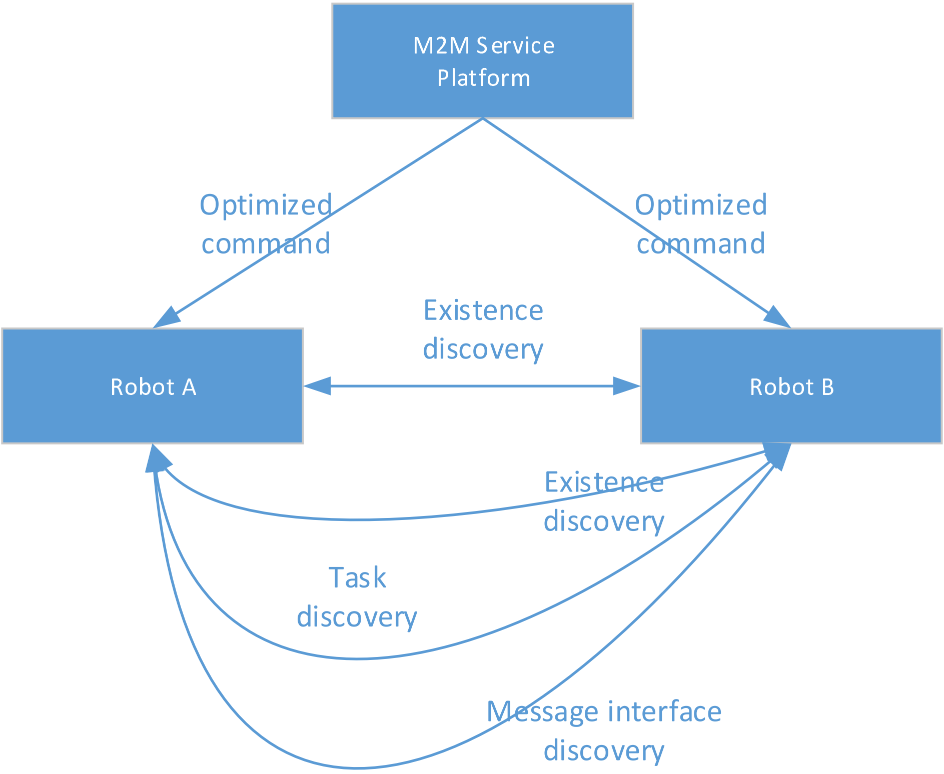

Figure 5.8.5.9-1: Machine Socialization

5.8.5.10 Use case analysis

IoT data that may compromise data usability:

- Capabilities of a Robot: when a robot is placed into service, if it does not describe its capabilities correctly then the overall service requests cannot be handled optimally by the cloud robot service platform.
- Status of a Robot: When reporting status, if the status is not described then the overall "user service request" cannot be completed.
- Cloud robot service platform commands: when a robot is commanded to perform a service, if the command is not recognized then the robot may not be efficiently utilized.

5.9 Retail Use Case

5.9.1 Use Case I.1: Retail inventory management

5.9.1.1 Description

Artificial intelligence can be used in retail to detect changes in inventory.

5.9.1.2 Source

Derived from various articles.

5.9.1.3 Actors

The presence of the following actors/entities as well as their associated roles are envisaged in the current use case:

- ***[Device]:*** sensors that can identify the presence and absence of a product in a retail environment.
- ***[Device]:*** AI/ML processing of sensor data.
- ***[Human]:*** A monitor, human or automatic, that can react based on the detected anomaly of a product inventory that needs replenishment.
- **Data user/consumer:** AI/ML Processing module, Monitor.

5.9.1.4 Pre-conditions

Products are able to be sensed in terms or absence or presence.

5.9.1.5 Triggers

The sensors measure aspects of the product being evaluated.

5.9.1.6 Normal flow

The AI/ML algorithm processes data from the sensors that detects when items are removed from their retail position. When a certain number of products are removed a signal or indicator is generated for the system operators to act upon to take an appropriate action.

5.9.1.7 Alternative flow

The AI/ML algorithm identifies that the sensors are not operating within normal parameters.

5.9.1.8 Post-conditions

Products that are not present in sufficient quantities are replenished to within normal parameters.

5.9.1.9 High Level Illustration

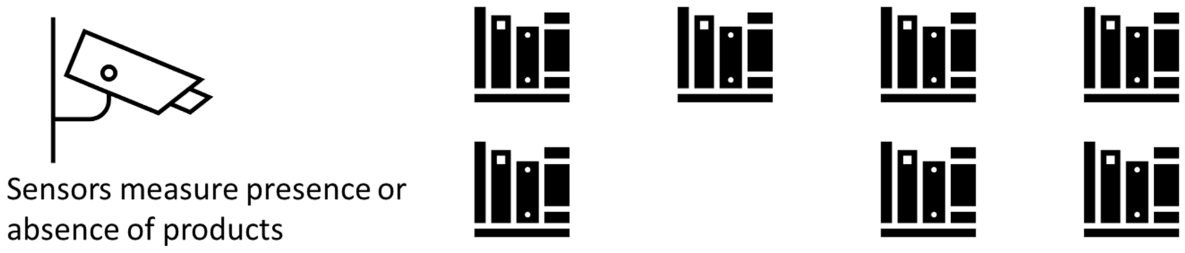

Figure 5.9.1.9-1: High Level Illustration of Retail Inventory

5.9.1.10 Use case analysis

Data that may compromise data usability:

- Incorrect sensor reading, for example a weight sensor, can lead to false indications by the AI/ML algorithm.
- Incorrect classifications from the AI/ML algorithm can lead to false "tasks or jobs" to replenish stock or failure to create a "replenish task/job".

Depending on the setting this could lead to expensive delays, in the case that a truck delivery has to be rescheduled, or not enough trucks allocated to the delivery task.

5.9.2 Use Case I.2: Vending Machines

5.9.2.1 Description

As part of the use case, the provider can limit access to availability of service for vending machines based on their geographic location. They can decide which area they would like to support service. The vending machine provider's does not want the vending machine users to move the machine from the specified area to other locations (potentially for better sales), hence, the providers can control the geographic distribution of their vending machines and make decisions based on data statistics and analysis (e.g. which are the best-selling areas? How many products are sold in specified areas during specified time? (and so on)).

5.9.2.2 Source

oneM2M TR-0001-Use_Cases_Collection [i.5].

5.9.2.3 Actors

- ***[Machine]:*** Vending machine, which can automatically sell products and report data information to the application platform through M2M service platform.
- ***[Machine]:*** The M2M service platform, which can control the vending machine device and its access to the network.
- ***[Machine]:*** Vending machine application platform, which can accept the data report from vending machine, monitor its status, and perform data analysis.
- ***[Organization]:*** Vending Machine Provider, make decision on the service.
- **Data user/consumer:** Vending Machine Provider.

5.9.2.4 Pre-conditions

The location information of the Vending machine is provided to the M2M Service platform by the Underlying network.

5.9.2.5 Triggers

- Vending machine restarts and registers to M2M service platform.
- Vending machine reports data information (e.g. each sale transaction or products selling information and so on).

5.9.2.6 Normal Flow

- The M2M service platform checks the geographic location policy. If current geographical location of the vending machine is in the permitted area, it allows the vending machine to register. Otherwise, it denies access which means customer is unable to get access to service.
- After vending machine successfully registers, it reports data information (for example, the product selling information and the stock information) periodically or for each product sale to the vending machine application platform through M2M service platform.
- The M2M service platform checks the geographic location policy. If the current geographic location of the vending machine is in the permitted area, it allows for the data report. Otherwise, it will be denied and service is unavailable.
- The vending machine application platform receives the data information report, records the information and performs data analysis.

5.9.2.7 Alternative Flow

None.

5.9.2.8 Post-conditions

N/A.

5.9.2.9 High Level Illustration

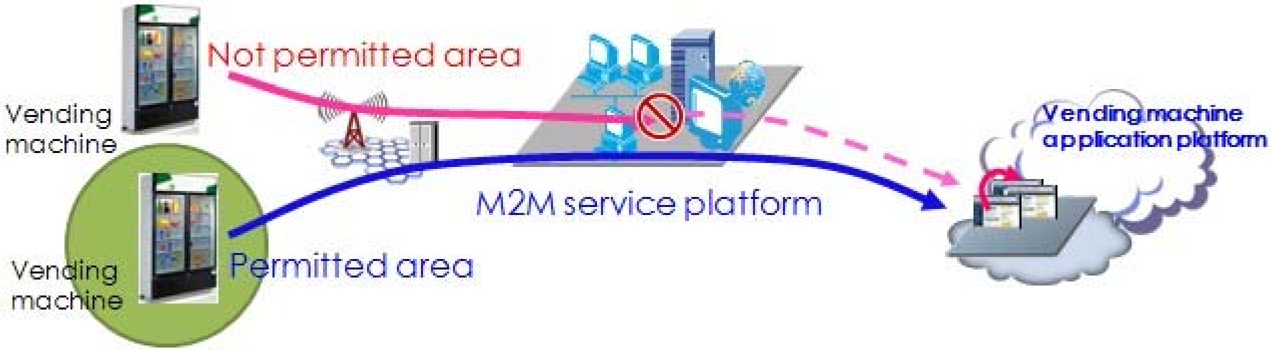

Figure 5.9.2.9-1: High level illustration of Vending Machines use case

5.9.2.10 Use case analysis

Data that may compromise data usability: Data from M2M application, that will include the sensor data about the wrong data information. Such wrong information can arise as a result of compromise to operation of the vending machine such that false sales are recorded to the M2M application platform. For example, some user may physically shake the machine and some products are available to users in which case it is not recorded as sales but it is not actually available for use. This wrong information may make the vending machine provider decide that the location of the machine remain in the area when it should not and there are no products available for consumption.

5.10 Large Events Use Case

5.10.1 Use Case J.1: Crowd Safety and Security

5.10.1.1 Description

This use case is about a cloud-based IoT platform supporting a series of applications that can be used to monitor, record and analyse the environment and consequently predict or identify situations which need attention in a large-scale event such as a concert. The use case relies on sensors generated by wrist band, CCTV camera, mobile phones, trackers and glasses, reporting data to an IoT cloud-based system, which handles incidents, supported by applications that help ensure efficient communication and a timely response. This use case is from the EU project MONICA [i.16].

During the event, the security personnel can monitor the situation using a web-based interface: the MONICA-COP provides an operational picture of the environment in real-time, and which displays notifications in case of any unusual activities. Furthermore, mobile apps for staff and visitors are also used for display and communication purposes.

The MONICA services include crowd and capacity monitoring, detection of security, health and safety incidents as well as location of and communication between staff, visitors and control centre.

5.10.1.2 Source

MONICA Project [i.16].

5.10.1.3 Actors

- ***[Human]:*** Event Staff/Organisers.
- ***[Human]:*** Events attendants.

- **Data user/consumer:** Event organisers.

5.10.1.4 Pre-conditions

As defined on the MONICA projects [i.16].

5.10.1.5 Triggers

As defined on the MONICA projects [i.16].

5.10.1.6 Normal flow

As defined on the MONICA projects [i.16].

5.10.1.7 Alternative flow

N/A.

5.10.1.8 Post-conditions

As defined on the MONICA projects [i.16].

5.10.1.9 High Level Illustration

As defined on the MONICA projects [i.16].

5.10.1.10 Use case analysis

Data that may compromise data usability: False readings from all or some of the sensors.

The applications are primarily based on data from CCTV cameras and crowd wristbands and these data can be compromised if for example the events attendants do not wear their wrist bands or readings are inaccurate. The consequence if the data is not correct means there could be a large number of crowds out of control and this could become unsafe in the context of large events like football games or concert.

5.11 Smart Lifts use case

5.11.1 Use Case K.1: Predictive maintenance and fault tolerance

5.11.1.1 Description

This case is about how the maintenance companies and technicians can use the available information to set a predictive maintenance program for the lift, and how they can use the remote connection with the lift to fix the faults or the problems.

Predictive maintenance is the "new" trend in lift industry even if it has been applied in several industrial sector for ages; the scope of predictive maintenance is to anticipate the event of a fault, evaluating the fault rate of the single components based on the number of runs of the lift. So, the maintenance companies can substitute the components before the fault arise and they can reduce the out of service for the lift.

With the remote connection between the lift and the technicians of the control cabinet supplier, the maintenance technicians can fix the fault very quickly (by an e-mail report or by a message sent automatically by the lift).

Furthermore, there are some faults very hard to discover and that require long time to be fixed, so the capability for the maintenance technician to have the direct and real-time support by the supplier technician could drastically reduce the out of service necessary to fix the fault.

5.11.1.2 Source

Derived from ETSI TR 103 546 [i.21].

5.11.1.3 Actors

- ***[Human]:*** Maintenance companies, which can automatically monitor the status of all smart lift installations and to check if there are potential undesired situations on some of them.
- ***[Human]:*** Maintenance technicians, which can receive a notice about a potential undesired event and can perform a preventive intervention over the smart lift installation.
- ***[Human]:*** Supplier technicians (especially of control cabinet), which can be involved in the maintenance operations based on the outcome of the data processing operation.
- System.
- **Data user/consumer:** Maintenance companies.

5.11.1.4 Pre-conditions

- The IoT devices and IoT service platforms are deployed and in operational condition.
- The data collection services are up and running.
- The Smart Lift is operational.

5.11.1.5 Triggers

- The data processing service detects a pattern having an over-threshold probability of leading to an undesired event.

5.11.1.6 Normal Flow

- The smart lift IoT ecosystem provides data to the remote central control unit installed within the Maintenance Company premises.
- The **remote central control unit AI** component detects a data pattern that, with a probability higher than a specified threshold, can lead to a possible fault or to an undesired event.
- The Maintenance Technicians are alerted about the undesired event together with the related explanation.
- The Maintenance Technicians check if the smart lift installation can be fixed by their own or if it is necessary to involve any Supplier Technicians team.
- The smart lift component is fixed or replaced.
- The smart lift installation restarts to work and the alert within the remote central control unit disappeared.

5.11.1.7 Alternative Flow

None.

5.11.1.8 Post-conditions

The smart lift component has been fixed or replaced and the data processing service does not alert about any possible undesired event.

5.11.1.9 High Level Illustration

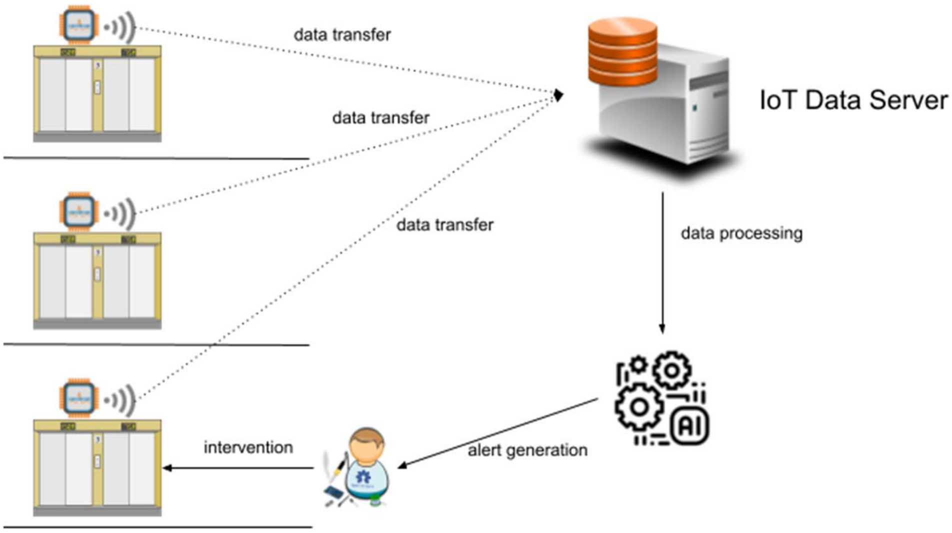

Figure 5.11.1.9-1:High level illustration of Smart Lifts - Predictive Maintenance use case

5.11.1.10 Use case analysis

A typical problem is that a fault appears but, when the maintenance technician is on site, the lift runs properly; this is a typical case of misuse by the users that some time smash the manual landing doors and the consequence is that the locking devices work sometime well and sometime badly.

In this case for the maintenance technician, it is very hard to discover the fault; the best solution is that the technician of the control cabinet supplier connects the lift from the remote position and analyses the faults; by the history of the faults recorded and the capability of analysing the single input and output of the main board, he can very quickly identify which landing door causes the fault and understand why the fault appears.

With predictive maintenance the system sends a message to the maintenance company that the lifetime of a component (for example: wheel of the doors, pushbutton, etc.) has expired; the maintenance company can send a technician to substitute the component with a new one, so the time of substitution could be very short and the possible out of service of the lift avoided.

Data that may compromise data usability:

- Data provided by IoT devices installed on each lift.

The whole predictive maintenance activity relies on the quality of the data provided by the IoT ecosystem to the main server. Any fault during the collection of such data (e.g. wrong read, network issue) can compromise the output of the AI-based predictive system by making it not usable for addressing the predictive maintenance task.

5.11.2 Use Case K.2: Low-connection environments

5.11.2.1 Description

This use case is inspired by the Lift Predictive Maintenance one with the difference that often, data produced by lift installations can only be saved, retrieved, and exploited locally due to, for example, a network connection that is not always one or given the high bandwidth cost. Indeed, while alarms and usage (number of rounds, maybe levels of rounds, power consumption) may be transmitted for remote maintenance, safety measurements and lift status remain local and, possibly, such information are saved for a few hours only.

This aspect opens to a more complex scenario where the entire end-to-end pipeline is decentralized and, by assuming to have a central data collector processing all produced data, reasoning and learning operation can be performed in a federated way.

The use case includes the necessity of design an architecture foreseeing a set of light-weight services that can be deployed and work on low-cost computational resources and a central repository able to aggregate federated learning models and in turn propagates new insights to all clients.

From the data usability perspective, in this use case the critical aspect is not related to the grant effective reading from IoT devices, but also to have an effective and efficient data transfer from each lift locations and the central data collector.

5.11.2.2 Source

Derived from ETSI TR 103 546 [i.21].

5.11.2.3 Actors

- ***[Human]:*** Lift companies, which can automatically monitor the status of all lift installations and to check if there are potential undesired situations on some of them.
- ***[Human]:*** The cloud data manager collects data from different installations deployed into low-connection environments it harmonizes the data with respect to a central data model.
- ***[Machine]:*** The decision support system processes collected data and generates reports and suggestions.
- ***[Human]:*** Maintenance suppliers, which can receive a notice about a potential undesired event and can perform a preventive intervention over the lift installations.
- **Data user/consumer:** Lift companies, Maintenance suppliers.

5.11.2.4 Pre-conditions

- The lift installation and IoT service platforms are deployed in an operational condition.
- The data collection services are up and running.
- The decision support system is operational.

5.11.2.5 Triggers

- The data processing service detects a pattern having an over-threshold probability of leading to an undesired event.
- The decision support system completed the generation of a report and/or was able to generate suggestions for optimizing the operational environment.

5.11.2.6 Normal Flow

- The lift IoT ecosystem provides data to the cloud data manager installed within the lift company premises.
- The lift IoT ecosystem provides data to the local data manager installed within the local environment.
- The cloud data manager collects data from different installations deployed into low-connectivity environments and it aggregates the data within a central data model.
- The decision support system connected to the cloud data manager detects a data pattern that, with a probability higher than a specified threshold, can lead to a possible fault or to an undesired event.
- The lift company is alerted and, in turn, it alerts the maintenance supplier about the undesired event together with the related explanation.
- The maintenance supplier checks if the lift installation has to be actually fixed.
- The lift component is fixed or replaced.
- The lift installation restarts to work properly and the alert within the remote central control unit disappeared.

5.11.2.7 Alternative Flow

None.

5.11.2.8 Post-conditions

The lift component has been fixed or replaced and the data processing service does not alert about any possible undesired event.

5.11.2.9 High Level Illustration

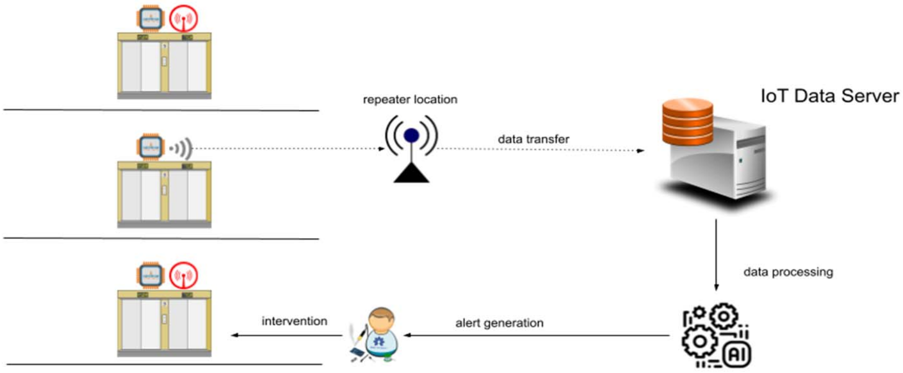

Figure 5.11.2.9-1: High level illustration of Smart Lifts - Low-connection environments use case

5.11.2.10 Use case analysis

Data that may compromise data usability:

- Data provided by IoT devices installed on each lift.
- Data stream network.

The risks connected with the data provided by the IoT devices are the same described in use case K.1. Hence, any service and activities relying on the quality of the data provided by the IoT ecosystem to the main server can compromise the processing activities of the AI-based predictive system by making it not effective for addressing the predictive maintenance task. In this specific use case, given the decentralization of the processing mechanism, the communication capabilities of the devices (and of the environment) is critical. Hence, issues during the data transferring activities (e.g. slow network during the communication task) can compromise the sending of information with the consequence of compromising the effectiveness of the whole system.

5.11.3 Use Case K.3: Building Manager

5.11.3.1 Description

Buildings administrators are interested to get information about some lift properties like power consumption during a specific timespan, how many times the lift has been called in each level, how many rounds the lift did, etc.

The data format produced by each lift may be different with respect to the lift's supplier. This means that if a building administrator is in charge of managing different building, it has to work with many different data formats making the decoding and the aggregation of the data quite laborious.

The analysis of such data is important for deriving and understand users' behaviour with the aim, for example, of improving the sustainability of building from cost perspective.

This use case is worthy of investigation for understanding (a) the type/format of data, and (b) their logic in order to infer behaviours by means of possible conceptual models. Homogeneity is needed to make the data collected easier to analyse, aggregate and be able to compare the information among different lift installations and reduce the out of service necessary to fix the fault.

This use case can be considered an abstraction of the use case described in use case K.1 where data produced by IoT devices are exploited by building managers for different purposes, e.g. energy saving, predictive maintenance.

5.11.3.2 Source

Derived from ETSI TR 103 546 [i.21].

5.11.3.3 Actors

- ***[Human]:*** Building manager, which can automatically observe the statistics about lift properties (e.g. power consumption and usage statistics).
- ***[Human]:*** Lift maintainer, which can update the functioning of lifts based on the requests coming from the building manager.
- ***[Human]:*** Cloud data manager, which is in charge of storing the heterogeneous data collected from different lift installation and to harmonize them with respect a common model.
- ***[Machine]:*** Decision support system, which can process collected data and to generate reports and to suggest optimization of lift's usage to building managers.
- **Data user/consumer:** Building manager.

5.11.3.4 Pre-conditions

- The IoT devices and IoT service platforms are deployed and in operational condition.
- The cloud data manager services are up and running.
- The decision support system is working.
- The lift is operational.

5.11.3.5 Triggers

The decision support system completed the generation of a report and/or was able to generate suggestions for optimizing the operational environment.

5.11.3.6 Normal Flow

- A lift installation (that can include one or more lifts) provides data to the cloud data manager.
- The cloud data manager collects data from different installations deployed into building managed by the same administrator and it harmonizes the data with respect to a common data model.
- The decision support system processes collected data and generates reports and suggestions.
- The building manager reads the report and analyses the suggestions before taking the decision about possible optimization that can be deployed.
- The lift maintainer updates the working software of the lift based on the suggested optimization.

5.11.3.7 Alternative Flow

None.

5.11.3.8 Post-conditions

The lift work in a more optimized way.

5.11.3.9 High Level Illustration

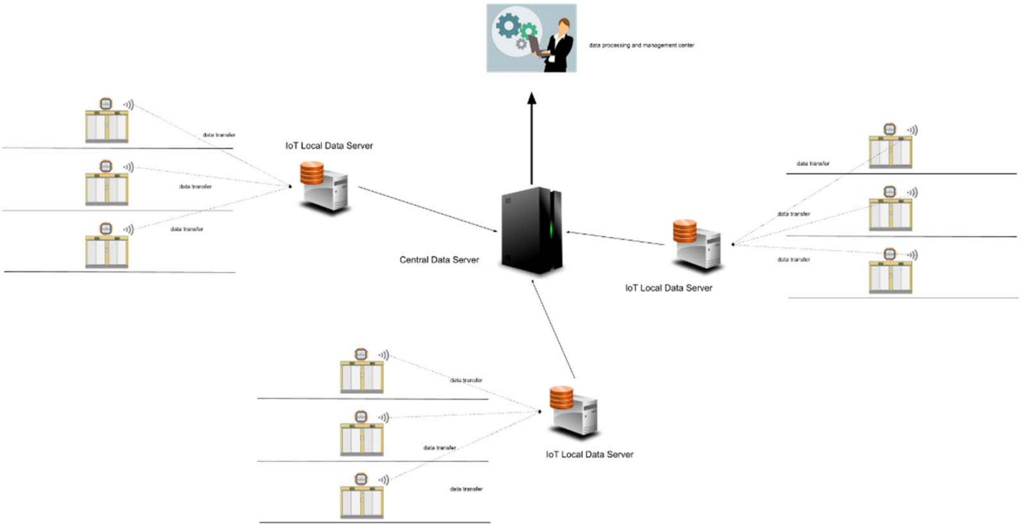

Figure 5.11.3.9-1: High level illustration of Smart Lifts - Building manager use case

5.11.3.10 Use case analysis

Data that may compromise data usability:

- Data provided by IoT devices installed on each lift.
- Data stream network.

The risks connected with this use case are very similar to the ones highlighted in both use cases K.1 and K.2. Indeed, the effectiveness of the AI-enabled system depends by the capability of IoT devices to provide correct values to the central data storage as well as to check if such data have been actually provided by avoiding network issues. Scenarios like energy saving, predictive maintenance, and usage optimization can be managed properly if all data generated by the IoT devices are properly stored within the central data storage. Given the distributed architecture, there is possibility that different data formats are used. Hence, the alignment through different versions of the data packages provided by the adopted IoT devices has to be foreseen.

5.12 Smart Cities use cases

5.12.1 Use Case L.1: Smart Lightning

5.12.1.1 Description

Beyond the use cases already described in the previous clauses (e.g. smart buildings, smart parking, the main use cases for smart cities are:

- Smart Lightning.
- Smart Waste.
- Environmental Monitoring.
- Digital city services and real-time dissemination of data shared between the city and the citizens.

The present clause discusses the smart lightning use case, which is described in more details in clause 8.1 "Street Light Automation" of oneM2M TR-0001[i.5], The objective is to appropriately modulate the street-level illumination according to weather conditions (clear, fog, rain, snow, etc.), time of day and the presence of people or vehicles. In addition, this use case may help improve the inhabitants' safety (sensitive areas get higher illumination), improve the city's maintenance operations and reduce the global energy consumption. This use case is under deployment in Chicago for example (see http://ChicagoSmartLighting.org).

In large cities, the IoT platform implementing this use case has to collect in real-time the data from thousands of different sensors located around the city, aggregate them and feed them to the AI process that takes the lighting decision.

Other use cases such as smart waste or environmental monitoring would lead to similar discussion in terms of data usability of the devices and the data they provide.

5.12.1.2 Source

oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

This use case is divided into several sub-use cases:

- Sub use case 1 - Local: Light sensors (detected light level).
- Sub use case 2 - Local: Light sensors (detected input voltage level).
- Sub use case 3 - Local: proximity sensors (civilian or emergency vehicles, pedestrians).
- Sub use case 4 – Operation Centre: Policies (regulatory & contractual).
- Sub use case 5 - Operation centre: Ambient light analytics (sunrise/sunset, weather, moonlight).
- Sub use case 6 - Operation centre: Predictive analytics (lights parts of streets predicted to be used).
- Sub use case 7 - From other service providers: Traffic light service input (emergency vehicle priority).
- Sub use case 8 - From other service providers: Emergency services input (vehicle routing, police action).
- Sub use case 9 - From other service providers: Road maintenance service input (closures and/or diversions).
- Sub use case 10 - From other service providers: Electricity service input (power overload).

5.12.1.3 Actors

- ***[Machine]:*** Street light automation application (service provider), has the aim to adjust street light luminosity.
- ***[Device]:*** Street light devices have the aim to sense, report, execute local and remote policies, illuminate street.
- **Data user/consumer:** Street light automation applications.

5.12.1.4 Pre-conditions

See oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

5.12.1.5 Triggers

See oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

5.12.1.6 Normal flow

See oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

5.12.1.7 Alternative flow

See oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

5.12.1.8 Post-conditions

See oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

5.12.1.9 High Level Illustration

See oneM2M TR-0001 [i.5], use case in clause 8.1 "Street Light Automation".

5.12.1.10 Use case analysis

Data that may compromise data usability:

- All the data collected by the sensors located around the city;
- Data provided by external sources: information about city events (planned and unplanned) that may require higher lighting while people are on the streets, information about public safety vehicles' path, power usage information from the smart grid.

The street light automation applications are typical "big data" applications. They should receive only useful, complete (e.g. no missing data in the flow) and non-redundant data (except where needed). The sensor location accuracy and maintenance are of prime importance. Due to the large amount of data to be collected, intermediate platforms aggregating the data from a selected location or selected type of sensors may filter unusual events and facilitate the decision-making process, by reducing its complexity. As in all AI use cases, the data presentation, format and meaning need to be clearly defined at all levels of the processing chain. Interoperability between the devices measuring the sensor data and the platforms aggregating and exploiting the data has a strong impact.

Lack of usability of the data or compromised data in this use case may have different consequences. It may result in a lack of safety in the city (criminal areas, vehicle accidents caused by inappropriate lightning). In most cases, it will only result in citizen's discomfort.

6 Analysis and Recommendation

6.1 Executive Summary of Study

A preliminary analysis shows that a common aspect needed for each use case is the process of setting up and configuration of the scenario described. Setup here means connecting a sensor to the cloud and then sending data to an AI/ML component for processing the data. Scenarios can exist where a single sensor can be used for multiple purposes, i.e. a camera observing traffic can be used for traffic congestion analysis as well as weather related road conditions. In this case the data from the camera could be processed by more than one ML algorithm and the resulting outputs could have different distribution or notification needs.

Related to setup, sensor data format should also be described. This has to be done for the sensor data and the input requirements for the AI/ML algorithms.

Additionally, a format of the output data needs to be described so that the consumers of the AI/ML algorithm can effectively process the data.

6.2 Summary Table

Table 6.1 describes the list of recommendations that may be addressed to handle some of the impact to issues raised under the use cases. The numbering below refers to numbers listed in table 6.1:

1) Setup: Easy way for sensor data to be directed to a user (human or ML algorithm).

2) Setup: describe data format such that it can be used without ambiguity by its intended user (human or ML algorithm).

3) Configuration: transform data, if necessary, for a ML algorithm input or human user installation.

4) Configuration: describe the sensor data quality, or suitability to use in different scenarios.

5) ML output: capture classification of ML algorithms along with the data of interest that generated the classification.

6) ML output: terms used for output: ontology for ML results.

7) ML output: organize output in a manner that is easy to find and understand "important" data without any ambiguity.

8) ML output: data duplication should be avoided, if possible, e.g. image from a camera is provided. Then it is "analyzed" 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".

9) ML output: identify the ML module used to provide a classification (traceability).

10) IoT system operation: timestamp and geolocate the data when necessary.

11) IoT system operation: ensure that data accessibility is enabled to all authorized users.

12) IoT system operation: ensure that data interoperability is enabled if data should be shared between different IoT systems.

13) IoT system operation: ensure that the system is properly maintained and default components can be easily identified.

14) Protect against privacy, security and data integrity breaches.

NOTE: Impact of Failure can be: High (H)/Medium (M)/Low (L).

6.3 Conclusion

The present document has documented a formal description of use cases in the different domains highlighted in the use cases and analysed the impact of these use cases from the data usability point of view.

It has identified, selected and described use cases where the IoT data and services require data usability specifications. It has also analysed the impact of these use cases for both machines and humans.

Potential solutions identified list of what can mitigate the identified issues with the intent of making the likelihood of the identified issue low. Each use case was looked at again to determine which potential solutions it might apply it to and then identified the residual impact assessment. The goal was to have the residual impacts for each use case become "Low". When all of the residual Impact assessments became Low, a subjective determination that the set of potential solutions has a reasonable level of completeness was derived.

Majority of the solutions identified in one way or another when addressed will improve the effect of data usability to the system. The table however suggests that the most common areas addressed include:

- Set up: this plays an important aspect to dealing with data usability issues.
- Configuration aspects: this should be considered and appropriate recommendation generated.
- ML output, IoT system operation and Privacy and security were also key but appeared less.

Some of the potential solutions are applied to many use cases and they will be further developed in a Technical Specification. There was however, one potential solution (#9: "ML output: identify the ML module used to provide a classification") that was not applied to any of the use cases, meaning that implementation of that potential solution did not address any of the identified issues. That does not mean that the potential solution is not useful, but rather that its benefit may occur in a different context.

Table 6.1

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
		Health Care					The application of these recommendations may reduce the risk to L.
A1	Adoption of an AI-based system for supporting patients.	Physicians, Patients, Users, AI engine.	Data provided explicitly by users. Data provided by IoT devices.	Indeed, the adoption of IoT technology can create new safety risks if it is not designed appropriately, implemented carefully, and used thoughtfully. Data integrity errors because of incorrect or missing data in the patient's Electronic Health Records (EHRs) and other health IT systems are a crucial issue in the healthcare sector that can dramatically affect patients (and users) health. Data integrity issues occurred with the use of paper medical records as well, but now, as EHRs become more interoperable and hackable, incorrect information is more readily available, more easily shared, and harder to eliminate. One patient's data appearing in another patient's record, missing data or delayed data delivery, and clock synchronization errors between medical devices and systems are examples of data integrity failures. These issues can lead to wrong inference or classification outcomes by the AI engine with the consequence of providing wrong information to the physicians and, even worse, compromising patient's health.	H	[2,3,4] The system has to be setup properly by taking into account the different data formats that can be exchanged by different devices. Indeed, the probability of integrating devices made by different manufacturers using, in turn, different data format is high. [10] Some devices can use both timestamp and geographic information for populating, for example, patient's PHR with physical activities information. It is necessary to verify that such metadata are properly and timely attached to the information generated by the devices. [11] The use of devices made by different manufactures means that there would be need of accessing to third-party systems. Hence, it is sensitive to verify that the ML system is	

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
						authorized to access such data.	
A2	Electronic Health records	Physicians, Patients, Healthcare Organizations, AI engine.	Information provided by clinicians. Device and IoT data (when used).	Information provided by clinicians are not properly stored into the system due to issues related to the format of such information or to some failures of the network. If IoT data are exploited, potential issues are linked to IoT devices that do not provide data according with the fine-grained level required or are not provided at all due to some failures. Moreover, the sensors can be affected by false reading issues than can affect the overall data usability of the patient's PHR.	H	Recommendations related to [2,3,4], [10], and [11] are inherited from the use case A1. [6,7] Information stored within each PHR has to be unambiguous since they can be read and manipulated also by humans. The use of common terminology is essential for making information understandable and usable. [14] PHRs contain patient's personal information. Depending on the type of user accessing such data, the privacy management facility has to manage the exposure of authorized data.	The application of these recommendations may reduce the risk to L.
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.

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
A4	Clinical intervention	Physicians, Patients, Healthcare Organizations, AI engine.	Information provided by patients (first case). Information provided by clinicians (first and second case). Device and IoT data (when used) (first and second case).	There are two possible scenarios that can be addressed within this use case. In the first one, the intervention is related to new behaviours that patients have to follow. Here, information provided by patients are crucial for keeping the AI system usable and effective. Instead, within the second scenario the AI is more invasive since the intervention includes surgeries. Here, the fine-grained level and the correctness of the data provided by sensors and actuators are crucial for avoiding dangerous issues. Together with the data provided by both sensors and actuators, also information provided by clinicians are critical as well since they are used for setting up the clinical intervention.	H	Recommendation [2,3,4] from use case A1, and recommendations [6,7] and [14] from use case A2 are inherited. [11,12] Invasive intervention may require the cooperation of different IoT devices. Hence, both the interoperability of the manipulated data format as well as the maintenance of the actuators have to be properly maintained for avoiding failures.	The application of these recommendations may reduce the risk to L.
		Public and Emergency Services					
B1	Automatic direct emergency call from IoT device.	The operator who handles IoT data received from the sensors. This operator may be human or an automatic process (AI).	Geolocation Alarms, Sensor data:a) In the case of the normal flow (nominal operation), data may be compromised if the system is not setup properly (location of the sensors is improperly configured) or the system maintenance is insufficient to ensure that the sensors are in working condition and do not trigger false positives.b) In the case of the normal flow (unsuccessful completion), the operator has been provided with two series	The consequences of failing this use case because the data became unusable at some point in time may be very important: forest, remote facility, building completely destroyed with potentially loss of human/animal lives.	H	[1] Setup: Data from the IoT platform should be easily understandable for a human operator monitoring the platform [3] Configuration: The location of the remote sensors should be reliable. [7] ML output: the alarm raised by the platform should be easy to understand without ambiguity by the system operator. [10 to 13] IoT system operation: all data should be properly timestamped and geolocated, to ensure	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
			of non-usable data that led to a disaster: • false alarms due to the lack of maintenance of the IoT platform and its sensors; • wrong location information of the first sensor (probably due the wrong configuration of the system).			traceability of the alarm. Maintenance should be performed periodically to verify the proper operation of the system.	
B2	Emergency services teams accessing pre-deployed IoT devices.	The emergency services who will use the data from the building system to make their operation more efficient.	Sensor data provided by the building IoT platform and their semantics. Problems that may arise: the emergency service team's devices are not compatible to data provided by the building's safety system; the emergency service team's devices misinterpret the data provided by the building's safety system which hinders the efficiency of the whole rescue operation. security authentication data that may prevent the emergency services from accessing and using the building data. Problems that may arise: the emergency service team's devices are not granted access by authenticating entity.	IoT data are usable in the case where their access is fully granted to people who may need to access them. Lack of interoperability at data level between systems (e.g. semantics unknown) may prevent ability to use these data by the emergency team. The consequences of failing this use case because the data are unusable as described above may be very important: building completely destroyed with potentially loss of human lives.	H	[6] ML output: the ML results when applicable should be unambiguous. [12] Setup. the data format should be understandable by the emergency team devices. [11,14] IoT system operation - privacy and security: the emergency team should be granted authorized access to the building data.	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
B3	Cooperative Fog Services with Drones.	Drone in role of Fog Node, Drone in Role of Fog Leader, User/Requestor of Fog services, IoT Service Layer Platform.	Fog node.	• Capabilities of a Fog node: when a device is included in the Fog, if it does not describe its capabilities correctly then the overall service requests cannot be handled optimally. • Status of a Fog node: When reporting status, if the status is not described then the overall "user service request" cannot be completed. • Fog node commands: when a device is commanded to perform a service, if the command is not recognized then the node may not be efficiently utilized.	M	[2,3,4] A concise and unambiguous description of the Fog Node capabilities, status and commands is required; alternatively the ability to convert a command from or to a device into a command that is used by the Fog leader or service layer.	L
		Industry and Manufacturing Use Case					
C1	Monitoring of industrial manufacturing equipment	The monitor, human or automatic.	Data coming from the sensors	If data are not generated normally (at the expected time intervals) or corrupted (fail to detect abnormal conditions), there is a risk that the machinery comprising the industrial production line could be damaged or the product that would be generated would be defective	M	[13] data from sensors should be analysed so that degradation of the sensor measurements (likely slow changes) are recognized and accounted for (calibration, replacement, etc.).	L
C2	Monitoring of industrial manufacturing products	A monitor, human or automatic	Sensor data.	This could result in defective products provided to consumers (for example, a bag of chips is not fully closed).	M	Same as C1.	L
C3	Link Binding in Digital Twins and Edge/Fog Computing	Resource Creator (logical entity)	Sensor data.	Sensors and Actuators attached to collect data in Physical part to create digital twin is corrupted either by link breaking or data collected is incorrect because of fault in sensors. These may result in wrong representation of physical product in digital form in real time as such the product is not being monitored or managed remotely. In situation where the product being manufactured is sensitive food, or children's toys this may lead to faulty batches that may compromise safety and lead to recall of product which may prove expensive	M	Same as C1 plus ensure that when the device is not connected the service layer can detect the disconnection and that data collected by the device is retained until connection is re-established and able to be successfully sent.	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
		ICT Network Management					
D1	Intelligent Software Rollouts	ENI system automation.	Report of the updating process.	User intervention may interrupt the automatic software update. Monitoring of data generated by sensors may produce inconsistency of results which may affect the retries of failed upgrade. Also forced user intervention whilst update is taking place may give false feedback that installation has been completed which may not be the case. The consequence of update not happening means that the software was not fully deployed properly and this is may not be detected, this suggests inconsistencies in all system and could mean unfruitful use of resources indirectly financial implication to organization.	M	[3,4] Configuration: If configured properly the ML algorithm can indicate unclear format, which can trigger alarm can be raised. Also, the type of data quality can be configured such that when this is not the case there can be an alarm raised for human intervention.	The application of this will reduce the risk impact to L.
D2	Policy-based network slicing for IoT security	ENI system automatic.	ENI monitoring data.	Potential error is if the ENI data collected from the websites or devices for example are corrupted in some way which means the ENI system is unable to detect that abnormal event has occurred (e.g. web site is no longer accessible, or the traffic patterns of a device do not correspond to its expected behaviour) and unable to carry out necessary analysis that determines if system is under attack or not. Data collected from devices should be available to the Network Administrator before analysis so if required there can be an intervention from the Network Administrator based on their own analysis.	M	[3,4] Configuration If configured properly the ML algorithm can indicate unclear format, which can trigger alarm can be raised. Also, the type of data quality can be configured such that when this is not the case there can be an alarm raised for human intervention. [7] ML output: organize output in a manner that is easy to find and understand "important" data without any ambiguity In this case the output data should be made available to the network administrator [human] in a format they can easily understand and detect the abnormal event.	The application of suggestion during configuration and also the format of output data into a human understandable format will reduce the risk of this happening. L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
D3	Personal data management mechanism based on user's privacy preference	Application Service Providers	Report of the updating process	The consequence of data not been usable means the data provided is incomplete when preference data is being configured in the PPM. It could also mean that during configuration of preferences that, connection is lost which leads to the data provided to the PPM for use by the Application Providers are compromised and this may lead to the wrong service being provided to the user resulting in misrepresentation of service.	M	[3,4] Configuration: If configured properly the ML algorithm can indicate unclear format, which can trigger alarm can be raised. Also, the type of data quality can be configured such that when this is not the case there can be an alarm raised for human intervention, incomplete data or format is not as expected. [1,2] Set up Setup: Easy way for sensor data to be directed to a user (humans are to check the service registered is what is expected) Also at setup: describe data format such that it can be used without ambiguity by its intended user [6,14] Check the terms used for output and also check that there are no privacy breaches	Application of these should reduce the risk to L
D4	Collection of M2M System data	Management platform, Monitor Centre, Data collection centre.	Definition of metrics collected by the M2M system.	Format and meaning of the Metric data provided to a M2M System Data Collection Centre has to be "understandable". If the information is not consistent there could be incorrect "insights" provided. For example, timestamps should have a defined and understandable format. Implementation of this use case can be used as a solution to detection of incorrect behaviour in other uses cases in the present document.	M	[2,3,4] Definition and description of key metrics (latency, throughput, memory usage, processor utilization, disk space, resource capabilities (CPU and memory speed), temperature).	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
						[13] processing times (and other characteristics such as system failures) of the M2M system can be used to identify potential errors of the M2M system itself.	
		Agriculture and Farming					
E1	Fertilization/Irrigation /Pest management service	Decision support system, Farmers.	Data provided by the satellite. Data provided by weather stations. Device and IoT data located in the field.	The decision support system is driven by the three types of data mentioned above. If one of the data sources fails to read the values or to provide them promptly, they would become not usable by the system with the risk of having an ineffective management of the farming system. In particular, the IoT devices located in the field are particularly exposed to adverse events (e.g. meteorological ones). This aspect can be mitigated by implementing a redundant network of sensors that can be used both as backup or as confirmation of the read values. This action would increase the overall data usability.	M	[2,3,4] The system has to be setup properly by taking into account the different data formats that can be exchanged by different devices. Indeed, the probability of integrating devices made by different manufacturers using, in turn, different data format is high. [10] Data provided by satellites and weather stations are all labelled with timestamp and geographic information. It is necessary to verify that such metadata are properly attached to the information provided to the ML component. [11] The use of devices made by different manufactures means that there would be need of accessing to third-party systems. Hence, it is sensitive to verify that the ML system is	The application of these recommendations may reduce the risk to L.

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
						authorized to access such data.	
		Mobility (Transportation)					
F1	Vehicle Diagnostic & Maintenance Report	Vehicle Owner, Vehicle Service Centre, Vehicle Detection M2M Application, Vehicle Service Centre technician.	• M2M device data provided to Vehicle Service Centre; diagnostics data provided to Vehicle Detection M2M Application. For example, sensor measurements describing the vehicle's operation may be taken at very high sampling frequencies. • Results of the maintenance evaluation which has to be statistically significant, e.g. at a 95 %. confidence level. • Diagnostic & Maintenance Report from Vehicle Resolution M2M application provided to Vehicle Owner: completeness of the vehicle-scanning report, user-friendliness of the defect-identification process, unambiguous identification of the documented vehicle.	The Applications behind the Vehicle Service Centre need to be able to clearly determine which parts need to be replaced. The data usability and easy understanding by humans of M2M device data is necessary (translation to natural language when relevant). In case of AI, data presentation and integrity are important to ensure a valid AI decision. Vehicle Owner (and the service technician) needs to understand how urgent the maintenance is, what needs to be replaced and which part needs to be changed. If the data is misleading, the technician may not be able to successfully perform the relevant maintenance. The mechanics (technician) needs also to 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 sensors) and to reset the condition that led to maintenance when it has been fixed. If the report is ambiguous, the mechanics may also order the wrong part. The consequences of failing this use case because the data were unusable may be very important: safety is not fulfilled in the vehicle, and it may lead to accident with potential loss of human lives.	H	[1] Setup: The sensor data should be accessible to their consumer (mechanics or ML algorithm). [4] Configuration: the sensor data confidence level should be known to enable proper diagnostic by the Vehicle Service Centre algorithm. [7] ML output. The content of the Vehicle Service Centre report should be unambiguous to enable proper maintenance of the vehicle. [10] IoT system operation: The data measured by the sensors should be time-stamped, for example to evaluate a potential repetition rate of the failure. [13] IoT system operation: The vehicle system should be properly maintained to prevent failure of the sensors.	L
F2	Smart Parking	Parking provider, billing	Status of parking lot, location of reserved	As an example, if the vehicle driver is provided with ambiguous or wrong information about available parking	M	[3] Configuration: the system should be	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
		provider, police centre for fining and vehicle driver.	parking area in the street, parking area cost and discount coupon, status of parking area (e.g. disabled-only) in the street and in the mall, vehicle plate information.	area information, he may park on a dynamically allocated disabled-only area or already reserved area and get fined. This may result from the wrong configuration of the service in case parking spots numbers in the IoT system do not match the actual parking spot locations. The use case also includes a sensor that reports illegal parking to police centre. The provided data should be accurate and delivered in a human-usable format to the policemen. The consequences of failing this use case because the data were unusable or ambiguous are moderate: a disabled person may not be able to park and go to the mall, the owner of another vehicle may be unduly fined. This is more about a bad quality service level.		properly configured to provide its data to the smart parking service (e.g. proper location and identification of each parking slot). [7] ML output. The information received by the driver should be unambiguous. [10] IoT system operation: The status of the parking spot should be recorded with a timestamp associated with the spot Identifier. [14] Privacy should be ensured for the vehicle owner.	
F3	Port automation: Tracking assets in terminal yard	Terminal management staff [Human]; Terminal Operating System (TOS) [Machine].	• Identification and location of CHEs and containers in the terminal yard. • Identification of other devices within the terminal yard. • Information about operation on containers handled by CHEs. • Route recording of every CHE with time and position of communication. • Timestamp and location of where the container is picked up and placed.	Location management should be done in a scalable manner as many objects need to be tracked reliably with position, identification, and timestamp. Data from all objects should be synchronized (e.g. identical time reference). Objects' position should be of sufficient precision. In this use case, the IoT system is constantly aware of the position of every CHE with an accuracy of ±0,5 m. The identification of each object (CHE, container, other devices in the terminal yard) should be unique to prevent invalid information and mishandling of containers. Lack of data usability in this use case may result in the loss of containers, which has mainly economic consequences.	M	[2,3] Setup Configuration: object identification data should be setup and configured properly to prevent mishandling of objects in the terminal field. [4] Configuration: The object's location should be of sufficient precision. [7] ML output: The TOS output should be easily understandable and highlight important data. [10] IoT system operation: each action and object measurement should also record its location and timestamp.	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
F4	Port automation: RTG remote control with Augmented Reality (AR) support	Terminal management staff, Remote RTG operator [Human]; Terminal Operating System (TOS) [Machine].	Video feed from RTG camera system, information about the location of containers within the terminal yard, TOS work orders, data from and commands for moving crane parts (hoist, gantry, straddle). Data from all objects should be synchronized (e.g. identical time reference). Objects' position should be of sufficient precision. Video feed from RTG camera system should be real-time with low latency. Work orders should be understandable by the TOS. Reporting from actions performed by the RTG should be reliable.	Lack of data usability in this use case may result in the loss of containers, which has mainly economic consequences. However, it may also have stronger consequences, but with very low probability, as a mishandled container may create an accident on the terminal yard with potential lives lost.	H	Same as use case F3 + [2] Setup: input to the ML should be understandable by the algorithm without ambiguity. [3] Configuration: all data samples should be synchronized to enable a proper operation of the algorithm. [14] Privacy should be ensured for the workers in the terminal field (camera system).	L
F5	Autonomous driving	IoT platform, Vehicle Driver, Autonomous driving application.	Sensor data, geolocation, instructions to driver or to actuators. These data may become unusable in many manners: There are low chances that sensors are improperly setup in the vehicle, but this may happen in the surrounding of the vehicle. But even the data generated by the vehicle sensor may become unusable if a sensor becomes defective. Checking and	Lack of data usability or compromised data in this use case may result in the lack of sufficient safety at the vehicle level, potential accident (e.g. the example of camera blinded by the brightness of the sun light which caused an accident by an autonomous car). This may result in some cases in the potential loss of human lives.	H	[2] Setup: data format for external objects on the road should be clearly defined. [3] Configuration: data from the different sources should be aggregated to fit into the ML algorithm. [4] Configuration: the data confidence level should be known to guarantee a valid evaluation by the ML algorithm. [10] IoT system operation: all data processed by the	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
			maintaining the IoT system in the vehicle is thus if primary importance. Applying lower confidence to data captured from the environment may be important as well. As in all mobility use cases, the objects position should be of sufficient precision to ensure valid decision making by the AI process and the ADApp. Ambiguous instructions to drivers and/or actuators, or failing to prompt the driver in a correct manner may result in both vehicle and driver wrongly relying on each other to cope with a safety issue. Finally, the AI process receives data from a very large number of sources. They should be clearly presented and if possible aggregated across the system to enable a smooth running of the AI process.			automated driving algorithm should have a valid timestamp. Geolocation should be available when necessary. [13] IoT system operation: the vehicle system should be maintained to prevent sensor failures. [14] Privacy should be ensured for the vehicle owner and the people in the vicinity of the car. The whole system should be highly secured.	
		Energy Use Case					
G1	Energy optimization using AI	ENI System	Data received from the virtual networks.	The data within ENI system is received from software sensors, however if the data is compromised as a result of corrupted sensor interface, the data is no longer usable by the machine or it could also mean that the machine process the wrong data to give false instruction indicating the power does not need to be switched to power save mode. Although this may not in itself be life threatening but it could mean the DC is not operating at its optimized level.	L	[1,2] Setup: The risk of this happening can be handled at the set up such that sensor data is to be directed to a ML algorithm, or that the sensor data is described in data	Risk is eliminated.

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
				The worst-case scenario could mean that a particular server is over used and may cause system to shut down and make service unavailable. Comment: the data are from software sensors but they still apply here when it comes to data usability.		format such that it can be used a ML algorithm, hence making sure the data quality is as expected. [5] Output ML output: by capturing the classification of ML algorithms along with the data of interest that generated the classification, could also in a format that human can interpret can help pinpoint where there is an error and this can be adjusted.	
		Building Use Case					
H1	Predictive Operations: Cleaning and waste removal notification service and warning.	Building Manager.	Data collected by sensor to indicate amount of time room was visited, e.g. door sensor, number of steps movement inside a building could be wrong if sensor is faulty.	These data can be sent to machine to analyse the threshold limit, and if this limit is reached falsely, this may mean that the rooms are not cleaned for the next users or the cleaners are called to clean when it is not needed and this will result in charging the business for work not needed.	L	[1,2] at set up all connected sensors are checked that they are giving data. [3,4] all sensors are configured to read data using the same metrics otherwise adjust to standard recognized by machine. [5,6,7] the output should be in format that human can be able to diagnose what the issue is.	With this applied the risk will be eliminated
H2	Building automation - Environmental	Building Managers.	Data collected by sensors to indicate the energy levels in rooms.	These data if false due to faulty sensor or wrong interval of measurement of sensors possibly during setup may indicate that the wrong temperature computed and this may lead to wrong adjustment of the temp in the building which may eventually lead to false alarm is raised.	M	[1,2] at set up all connected sensors are checked that they are giving data. [3,4] all sensors are configured to read	With this applied the risk is now L.

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
	monitoring.					data using the same metrics otherwise adjust to standard recognized by machine. [5,6,7] the output should be in format that human can be able to diagnose what the issue is.	
H3	Building automation - Home Energy Management.	Home User.	Data collected by sensors to indicate the energy levels in rooms.	These data if false may indicate that the wrong information is submitted to the EGW and leads to false adjustment of appliance which could be harmful and unsafe, another scenario is if the appliance does break, it can become expensive especially if this happens on a frequent basis.	L	[1,2] at set up all connected sensors are checked that they are giving data. [3,4] all sensors are configured to read data using the same metrics otherwise adjust to standard recognized by machine. [5,6,7] the output should be in format that human can be able to diagnose what the issue is.	The risk will be eliminated once this risk is applied.
H4	Smart safety of workers at building constructionsite.	OSH manager [Human]; BIM system [Machine].	Location and proximity data of workers on site, physiological parameter measurements, weather conditions measurements, personal identification information, training and medical records, building information, user's thermal comfort preferences, alerts and notifications. Location data should be of sufficient precision and reported in real-time.	Lack of data usability or compromised data in this use case may result in restricted safety for the site workers, which may have strong consequences in case of false negatives (unhealthy conditions are not detected) or invalid navigation instructions that drive the worker to a hazardous area. If the consequence if raising false positives, the impact is mostly lower, just leading the worker to be further screened while there is no issue.	H	[2,7] Setup ML output: data at input and output of the BIM should be easily captured and understandable by the site workers. [3] Configuration: external data, such as weather conditions should be transformed to be captured by the BIM algorithm. [4] Configuration: the location data should be of sufficient precision.	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
			User interface in construction worker's device should be easily understandable, whatever the language and reading level of the worker. Reporting should be relevant to enable fast decisions as needed by OSH manager. Data flow from all devices should be secured and respect privacy, as well as guarantee data integrity. The BIM should be setup without any ambiguity or invalid information, as this may lead to invalid navigation and put the workers at risk. Clarity of navigation instructions based on user feedback.			[10] IoT system operation: all data processed by the BIM algorithm should have a valid timestamp. Geolocation should be available when necessary. [14] Privacy should be ensured for the workers on site affected by the BIM. The data flow on site should be secured.	
H5	Machine socialization	Cloud Robot service platform.	Capabilities of Robot Status of Robot Cloud Robot System.	• Capabilities of a Robot: when a robot is placed into service, if it does not describe its capabilities correctly then the overall service requests cannot be handled optimally by the cloud robot service platform. • Status of a Robot: When reporting status, if the status is not described then the overall "user service request" cannot be completed. • Cloud robot service platform commands: when a robot is commanded to perform a service, if the command is not recognized then the robot may not be efficiently utilized.	M	[2,3,4] A concise and unambiguous description of the robot capabilities, status and commands is required; alternatively, the ability to convert a command from or to a device into a command that is used by the cloud robot service or service layer.	L
		Retail Use Case					
I1	Retail inventory management	AI/ML Processing module, Monitor.	Incorrect sensor reading, for example a weight sensor, can lead	Depending on the setting this could lead to expensive delays, in the case that a truck delivery has to be rescheduled, or not enough trucks allocated to the delivery task.	L	[13] data from sensors should be analysed so that degradation of the sensor measurements	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
			to false indications by the AI/ML algorithm. Incorrect classifications from the AI/ML algorithm can lead to false "tasks or jobs" to replenish stock or failure to create a "replenish task/job".			(likely slow changes) is recognized and accounted for (calibration, replacement, etc.).	
I2	Vending Machines	Vending Machine Provider.	Data from M2M application	Data from M2M application, that will include the sensor data about the wrong data information. Such wrong information can arise as a result of compromise to operation of the vending machine such that false sales are recorded to the M2M application platform. For example, some user may physically shake the machine and some products are available to users in which case it is not recorded as sales but it is not actually available for use. This wrong information may make the vending machine provider decide that the location of the machine remain in the area when it should not and there are no products available for consumption.	L	[1,2] at set up all connected sensors are checked that they are giving data. [3,4] all sensors are configured to read data using the same metrics otherwise adjust to standard recognized by machine. [5,6,7] the output should be in format that machine can be able to diagnose what the issue is.	The risk will be eliminated once this risk is applied
		Large Events Use Case					
J1	Crowd Safety and Security	Event organisers.	False readings from all or some of the sensors.	The applications are primarily based on data from CCTV cameras and crowd wristbands and these data can be compromised if for example the events attendants do not wear their wrist bands or readings are inaccurate. The consequence if the data is not correct means there could be a large number of crowds out of control and this could become unsafe in the context of large events like football games or concert.	M	[1,2] at set up all connected sensors are checked that they are giving data.[3,4] all sensors are configured to read data using the same metrics otherwise adjust to standard recognized by machine.[5,6,7] if the data is not usable for example if the wrist bands are not worn properly, then notification can be sent to the users to check the band maybe	Once this has been applied the risk is reduced but not eliminated as there will be some users that will not apply the wrist band properly in which case nothing can be done. Risk L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
						through phone call they used during registration. Also the notification can be repeated for a set period until its defined that the sensor can be taken out of the equation. [8,14] The output should be checked that privacy and security of output data should also be checked that this are not compromised at any time.	
		Smart Lifts use case					
K1	Predictive maintenance and fault tolerance	Maintenance companies.	IoT devices do not provide data according with the fine-grained level required or are not provided at all due to some failures.	Maintenance team cannot intervene timely for avoiding out of service events of the monitored lifts. Moreover, the maintenance company is not able to understand which is the status of each lift.	H	[2,3] The system has to be setup properly in order to be sure that all data are produced and properly transformed into a usable format. [10] IoT sensors installed on each lift produce data that are labelled with timestamp information. It is necessary to verify that such values are properly attached to the information generated by the devices. [13] Given the sensitivity of the IoT sensors role, the system has to be periodically checked and maintained in	The application of these recommendations may reduce the risk to L.

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	**Use Case**	**Data Owner**	**Data that may be compromised**	**Consequence**	**Impact of Failure (H/M/L)**	**Recommendation**	**Residual Impact after Recommendation**
						order to avoid data loss.	
K2	Low-connection environments	Lift companies, Maintenance suppliers.	IoT devices do not provide data according with the fine-grained level required or are not provided at all due to some failures. Moreover, the sensors can be affected by false reading issues given by the interruption of connection. Finally, some data could be lost due to cache issues within the IoT devices.	The maintenance suppliers do not receive complete information from each remote lift. Hence, collected data are partial and not usable from the ML for estimating possible point of failures and, at the same time, they are not usable from the maintenance suppliers for understanding lift's status.	H	Recommendations from use case K1 are inherited. [8] Working with data transfer operations that can be interrupted due to connection issues may lead to data duplication. It is necessary to carefully check that data transmitted after a connection lost are not re-transmitted. This aspect may compromise the usability of the data from the ML component.	The application of these recommendations may reduce the risk to L if some actions are performed for enhancing network facilities within the affected building.
K3	Building Manager	False readings from all or some of the sensors.	Data are lost during the transfer from a building and the central data cloud storage. Issues related to data reading from IoT devices are inherited from use cases K1 and K2.	The building manager is not able to optimize the work of the lifts located within a specific building with the consequence of having a resource consumption higher than expected. Moreover affected lifts will not work in an optimal way for serving people.	M	Recommendations from use cases K1 and K2 are inherited. [10] Recommendation described within the use case K1 is extended to the use of geographic information since lifts are distributed across several buildings.	The application of these recommendations may reduce the risk to L.
		Smart Cities use cases					
L1	Smart Lightning	Street light automation applications	All the data collected by the sensors located around the city; Data provided by external sources: information about city events (planned and unplanned) that may require higher lighting	The street light automation applications are typical "big data" applications. They should receive only useful, complete (e.g. no missing data in the flow) and non-redundant data (except where needed). The sensor location accuracy and maintenance are of prime importance. Due to the large amount of data to be collected, intermediate platforms aggregating the data from a selected location or selected type of sensors may filter unusual events and facilitate the decision-making	H	[2] Setup: the deployed system should be scalable, accepting inputs from all sorts of sensors. [3] Configuration: data from different data sources should be understandable by the	L

The numbers referenced within the table correspond to the numbers mentioned in clause 6.2							
Use Case#	Use Case	Data Owner	Data that may be compromised	Consequence	Impact of Failure (H/M/L)	Recommendation	Residual Impact after Recommendation
			while people are on the streets, information about public safety vehicle's path, power usage information from the smart grid,	process, by reducing its complexity. As in all AI use cases, the data presentation, format and meaning need to be clearly defined at all levels of the processing chain. Interoperability between the devices measuring the sensor data and the platforms aggregating and exploiting the data has a strong impact. Lack of usability of the data or compromised data in this use case may have different consequences. It may result in a lack of safety in the city (criminal areas, vehicle accidents caused by inappropriate lightning). In most cases, it will only result in citizen's discomfort.		smart Cities algorithms. The data should be transformed and/or aggregated, as necessary. [4] Configuration: The events and objects' location should be of sufficient precision. [10] IoT system operation: all data processed by the smart city system should have a valid timestamp. Geolocation should be available when necessary. [13] IoT system operation: the smart city system should be maintained to prevent sensor and device failures.	

Annex A:
Change History

Date	Version	Information about changes
04-2021	0.0.2	Early draft uploaded for TC SmartM2M Ad-hoc meeting>
05-2021	0.0.3	Updated version of early draft uploaded for TC SmartM2M #58
07-2021	0.0.4	Stable draft uploaded for TC SmartM2M Ad-hoc meeting
07-2021	0.0.5	Updated version of V0.0.4 where two irrelevant use cases were removed
09-2021	0.0.6	Updated stable draft uploaded for TC SmartM2M #59
09-2021	0.0.7	Pre-final draft uploaded for comments from TC SmartM2M
10-2021	0.0.8	Final draft for approval uploaded for TC SmartM2M Ad-hoc meeting
11-2021	0.0.9	Final draft for approval revised following comments from TC HF
11-2021	1.1.1	ETSI Technical Officer review before publication pre-processing by ***editHelp!*** after SmartM2M TB Approval

Annex B: Bibliography

- ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

- IEEE Communications Survey: Deep Learning in Mobile and Wireless Networking: A Survey (IEEE Communications Surveys & Tutorials, March 2019).

NOTE: Available at 1803.04311.pdf (arxiv.org).

- ITU-T, FG ML5G use cases: "Machine learning in future networks including IMT-2020: use cases" (ITU-T, Supplement 55 to Y.3170 Series, October 2019).

History

Document history		
V1.1.1	December 2021	Publication