ETSI TR 104 411 V1.1.1 (2026-07)

TECHNICAL REPORT

Data Solutions (DATA);
Pandesys use cases and requirements

Reference
DTR/DATA-00104411

Keywords
ACT, IoT, semantic, use cases

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Data Solutions (DATA).

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.

1 Scope

The present document identifies meaningful eco-bio emergencies use cases that cannot be captured by ETSI TS 103 757 [i.3] using oneM2M as the IoT inter-connexion framework. In particular real-time, forecasting, and identity issues will be focused.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.2] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.3] ETSI TS 103 757: "SmartM2M; Asynchronous Contact Tracing System; Fighting pandemic disease with Internet of Things (IoT)".

[i.4] ETSI TR 103 509: "SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well".

[i.5] ETSI TR 103 510: "SmartM2M; SAREF extension investigation; Requirements for Wearables".

[i.6] ETSI TR 103 582: "EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations".

[i.7] ETSI TR 118 501: "oneM2M Use Case collection".

[i.8] Luigi Liquori and Egan Perais: "oneM2M Executive Viewpoint series: interview Luigi Liquori (Inria)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACT	Asynchronous Contact Tracing
AI	Artificial Intelligence
IoT	Internet of Things
PAMAC	Patrolling and Monitoring Administration Centre
ROV	Remoted Operated Vehicles
UxV	Unmanned x Vehicles

4 Background

4.1 Motivation

ETSI TS 103 757 [i.1] (Asynchronous Contact Tracing (ACT)) was conceived in opposition with synchronous contact tracing protocols, the latter tracking two individuals on the basis of the anonymous transmission of the identities of two mobile phones staying in the range of 2 meters for at least 15 minutes, but relying on the fact the one of the two individual, when infected, notifies its illness to the tracking system, notification that was largely disattended because of social fears.

ACT takes the contact tracing from another point that could be resumed as follows:

1) using IoT sensors to record viruses, called Detection Services;

2) equip them with a uniquely identified ID;

3) broadcast the ID using a Peripheral Service (e.g. Wi-Fi® transmitter); and

4) communicate the virus results to a Base Control Station Service thought an intermediary Local Service to load balance the message charge.

An human, usually equipped with a smartphone in its pocket, can continuously listen and record the IDs related with the position he visited, but he will never communicate anytime anywhere such information (hence its name, asynchronous). The user can at any time query the Base Control Station Service about the virus status in a geographic area recorded by one or more ID-Detection Service and eventually match those IDs with the footprint recorded in its Smart Mobile Application: in case of non-empty intersection, he will take countermeasures.

Figure 4.1-1 resume the mapping of ACT in the common oneM2M framework.

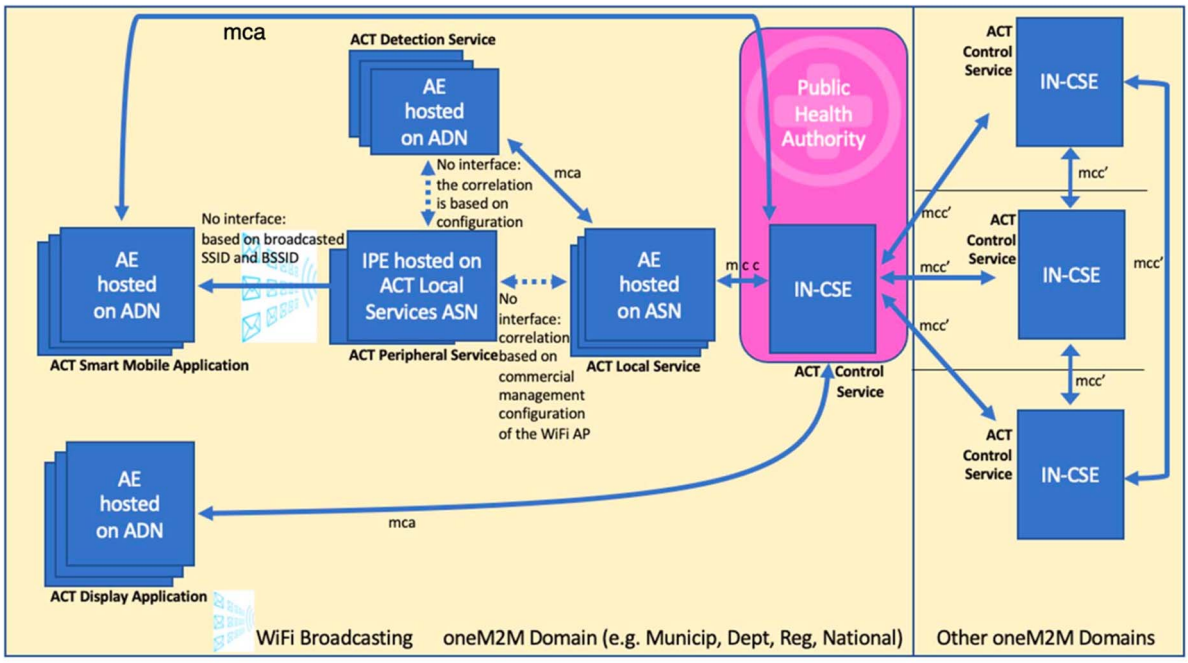

Figure 4.1-1: Mapping of the ACT Architecture in the common oneM2M Framework

4.2 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 concerning their exploitation within an ACT system.

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

- Health Care.
- Public and Emergency Services.
- Industry and Manufacturing.
- Agriculture and Farming.
- Energy.
- Smart Cities.
- Patrolling.

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 details in ETSI TR 103 533 [i.1] and ETSI TR 103 591 [i.2]. 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 citizens

5.1.1.1 Description

- Citizens may be exposed to communicable disease pathogens that may affect their health.
- A user may need to know if she passed through a certain area during a specific timeframe.
- IoT network detects the presence of specific pathogens.
- A user should be able to provide anonymous information concerning the presence of a specific pathogen within a given area.
- A user should be able to define a geographical area and a time period and then to search for data related to such area-time combination.

5.1.1.2 Source

- ETSI TR 103 509 [i.4].
- ETSI TR 103 510 [i.5].

5.1.1.3 Actors

- ***[Human]*** Physicians.
- ***[Human]*** Citizens.
- ***[Human]*** Users.
- ***[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

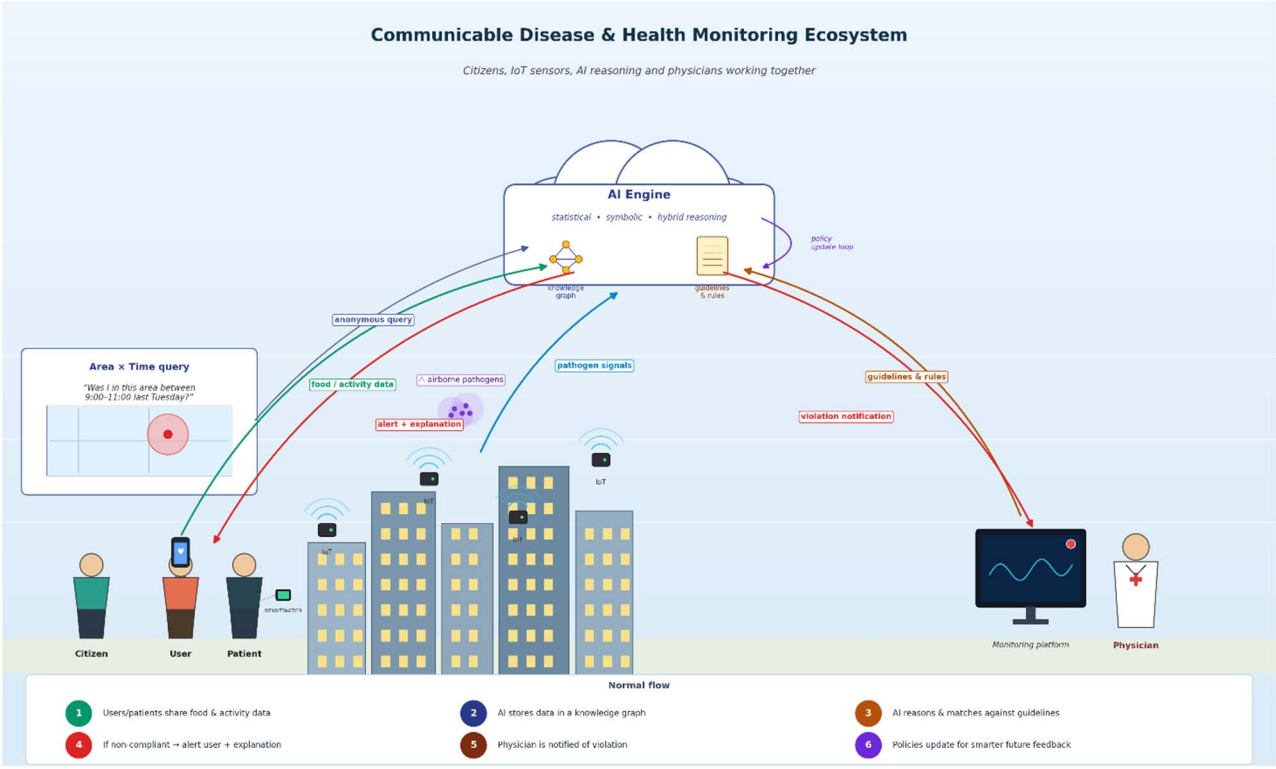

Figure 5.1.1.9-1: High level illustration of the described use case

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 patients' 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

5.2 Public and Emergency Services Use Cases

5.2.1 Use Case B.1: Detection of emergency signals from IoT device

5.2.1.1 Description

- Emergency personnel may need to detect which IoT device emitted an emergency signal within a specific area.
- A user may need to know if she passed through an area, where an emergency signal has been triggered, during a specific timeframe.
- A user should be able to provide anonymous emergency signals.
- A user should be able to define a geographical area and a time period and then to search for data related to such a area-time combination.

5.2.1.2 Source

Derived from ETSI TR 103 582 [i.6], EC1: 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

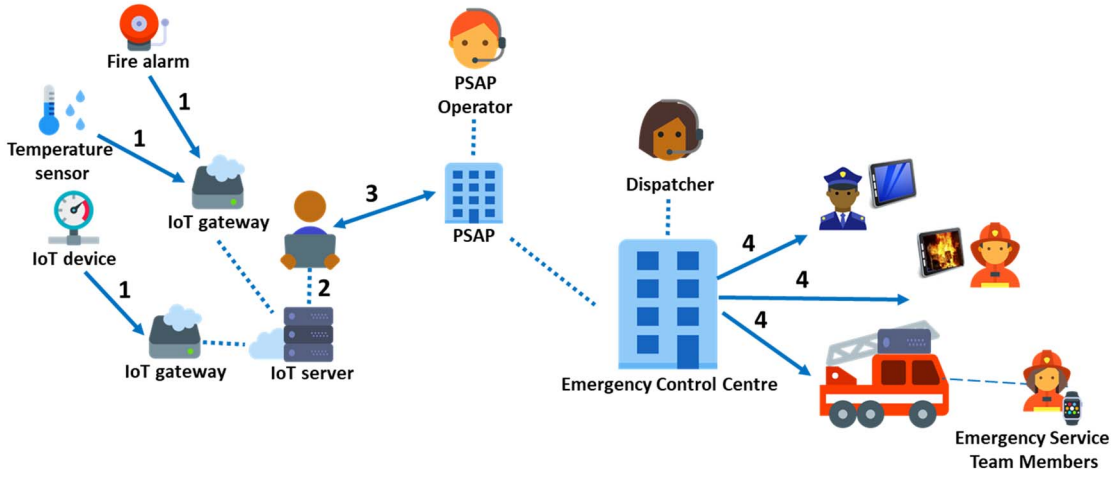

Figure 5.2.1.9-1: Illustration of automatic emergency call from IoT device

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.3: Cooperative Fog Services with Drones

5.2.2.1 Description

- Service personnel may need to detect areas where drones are flying to collect data under fog emergency.
- A user may need to query real-time and/or historical data provided by drones within a specific area.
- A user should be able to provide anonymous data from fog-affected areas.
- A user should be able to define a geographical area and a time period and then to search for data related to such a area-time combination.

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.

5.2.2.2 Source

ETSI TR 118 508 [i.7], clause 12.27.

5.2.2.3 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.

5.2.2.4 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.

5.2.2.5 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.

5.2.2.6 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.

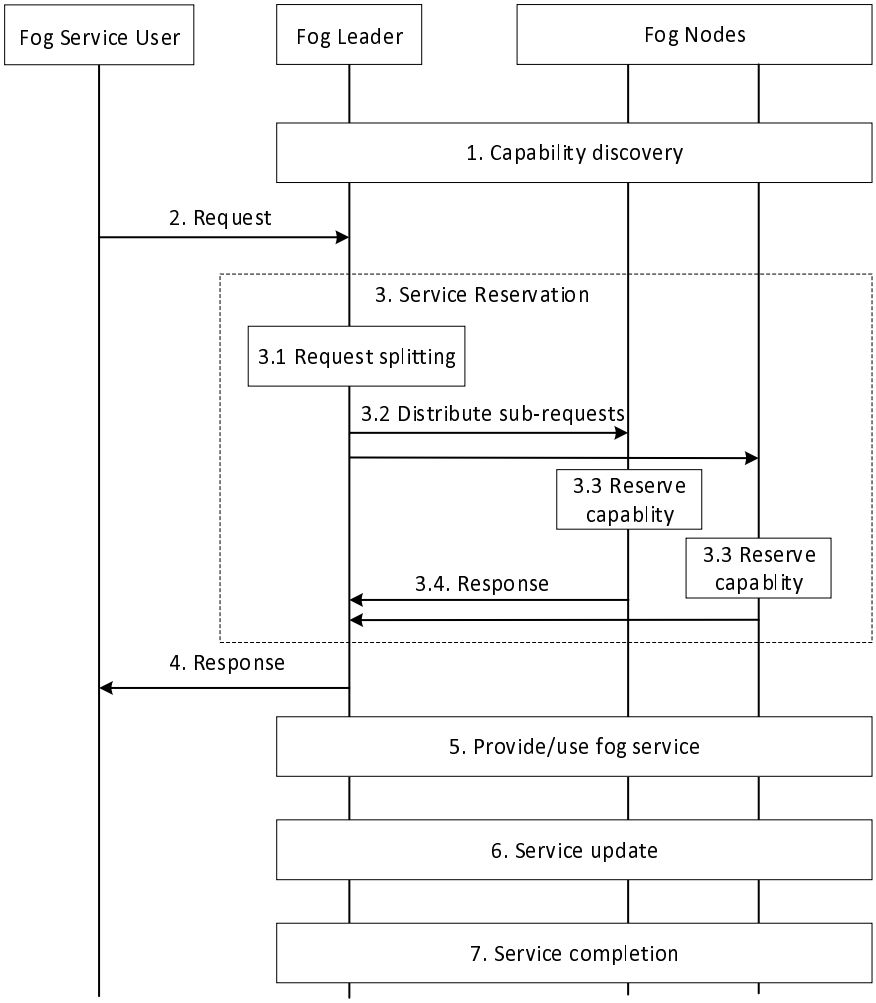

Figure 5.2.3.6-1: Normal Flow - Cooperative fog service

5.2.2.7 Alternative Flow

None.

5.2.2.8 Post-conditions

N/A.

5.2.2.9 High Level Illustration

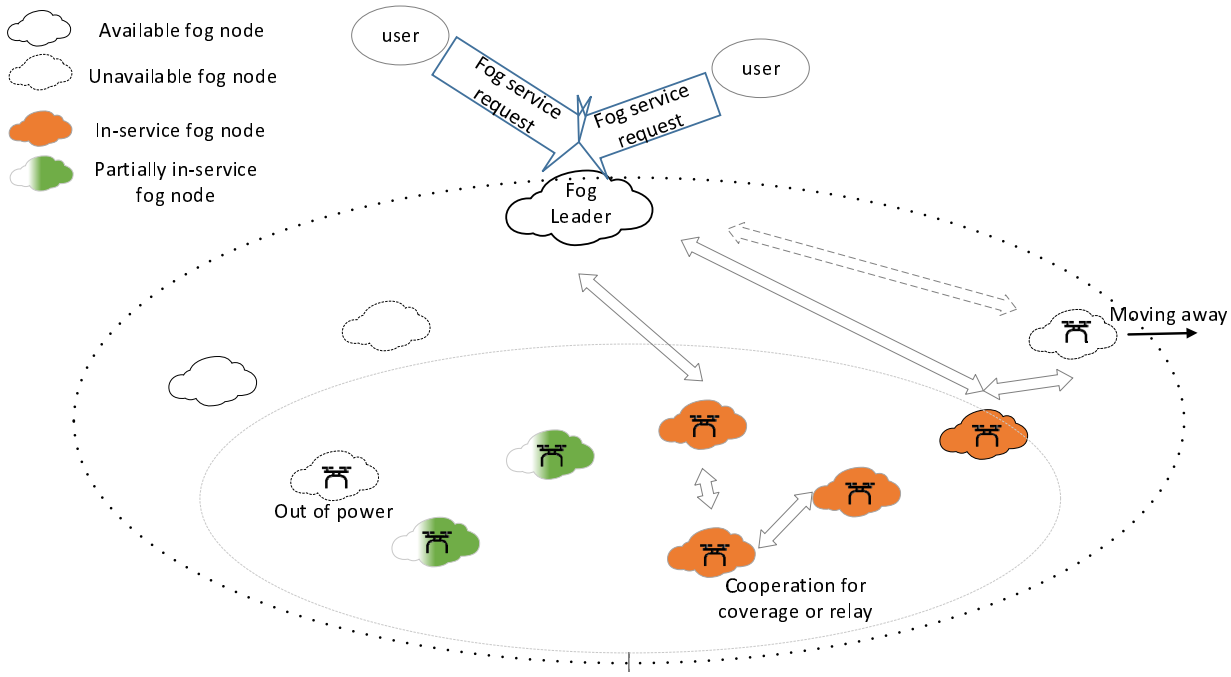

Figure 5.2.3.9-1: High Level Illustration - Cooperative Fog Service

5.2.2.10 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 Agriculture and Farming

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

5.3.1.1 Description

- Citizens may be exposed to toxic compounds that may affect their health.
- A user may need to know if she passed through a certain area during a specific timeframe.
- A user should be able to provide anonymous information concerning the presence of a specific chemical compounds within a given area.
- A user should be able to define a geographical area and a time period and then to search for data related to such a area-time combination.

5.3.1.2 Source

Internet of Farming H2020 project (IoF2020 - Grant number 731884): D3.5: Guidelines for the use of IoT related Standards in Smart Farming and Food Security

5.3.1.3 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.

5.3.1.4 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.

5.3.1.5 Triggers

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

5.3.1.6 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.

5.3.1.7 Alternative flow

None.

5.3.1.8 Post-conditions

The fertilization and irrigation system is calibrated properly.

5.3.1.9 High Level Illustration

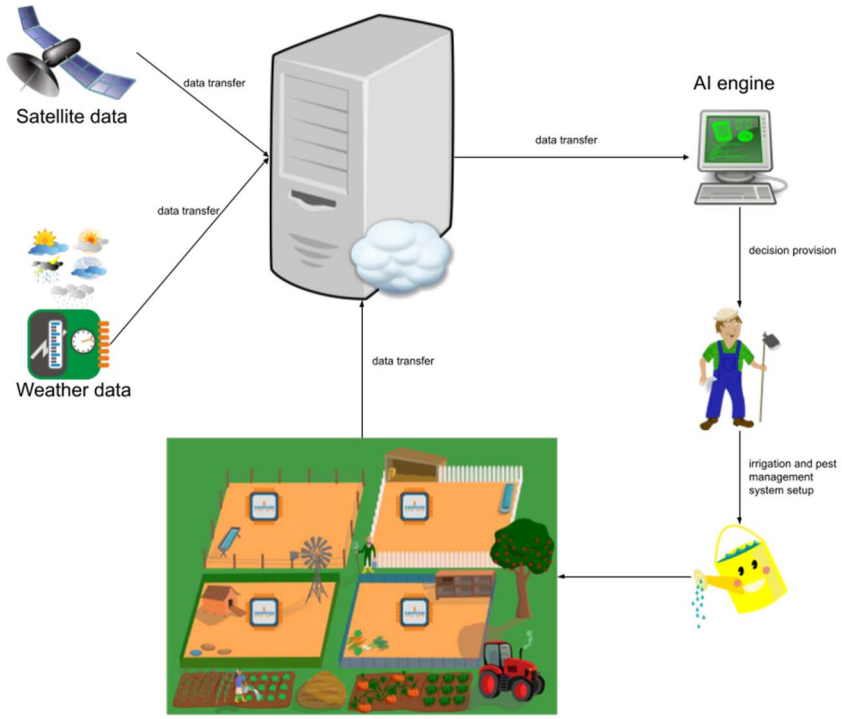

Figure 5.3.1.9-1: High level illustration of Smart Agriculture - Fertilization/Irrigation/Pest management service use case

5.3.1.10 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.

5.4 Smart Cities use cases

5.4.1 Use Case L.1: Smart Lightning

5.4.1.1 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 ETSI TR 118 501 [i.7]. 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.

5.4.1.2 Source

ETSI TR 118 501 [i.7], 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).

5.4.1.3 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.

5.4.1.4 Pre-conditions

See ETSI TR 118 501 [i.7], use case in clause 8.1 "Street Light Automation".

5.4.1.5 Triggers

See ETSI TR 118 501 [i.7], use case in clause 8.1 "Street Light Automation".

5.4.1.6 Normal flow

See ETSI TR 118 501 [i.7], use case in clause 8.1 "Street Light Automation".

5.4.1.7 Alternative flow

See ETSI TR 118 501 [i.7], use case in clause 8.1 "Street Light Automation".

5.4.1.8 Post-conditions

See ETSI TR 118 501 [i.7], use case in clause 8.1 "Street Light Automation".

5.4.1.9 High Level Illustration

See ETSI TR 118 501 [i.7], use case in clause 8.1 "Street Light Automation".

5.4.1.10 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.

5.5 ROP - UxV Patrolling

5.5.1 Description

Remoted Operated Vehicles (ROV) and Unmanned x Vehicles (UxV) (with x in {A,U,G} for Aerial, Underwater, and Ground) are two classes of vehicles, human or autonomous driven, that can be equipped with IoT and M2M technology. They are essentially **mobile entities** that can be instrumented with different sensors and actuators. This case study cannot be captured by [i.3].

5.5.2 Source

Inspired to the case studies presented in the Patrolling and Monitoring Administration Center (PAMAC) designed at Inria and at the University of Udine [i.8]: it represents a standardized approach to autonomous vehicle fleet management and coordination for surveillance and monitoring applications. PAMAC enables seamless interoperability between heterogeneous autonomous vehicles from different manufacturers, addressing critical gaps in current systems including lack of standardization, limited multi-vehicle coordination capabilities, and insufficient support for mixed fleets.

5.5.3 Actors

- ***[Human]*** Owners equipped with a Smart Mobile Application.
- ***[Devices]*** ROV - UxV equipped with a Detection Service and a Peripheral Service broadcasting an ID: devices are mobile and they can be remotely controlled or autonomous; devices are equipped with **sensors and actuators**, and they can interact each other.

- ***[Devices]*** ROV - UxV equipped with a Smart Mobile Application: devices are mobile, they can record their **footprint**, and they can interact each other.
- ***[Machine]*** New ACT platform monitoring the status of the **mobile** sensors and actuators and providing a control console Decision Support System, which is in charge of **collecting** all the data, **analyse** them and provide **forecasting** in case of queries concerning the future.

5.5.4 Pre-conditions

- ROV - UxV are devices are deployed.
- Almost (but not all) ROV - UxV can communicate and are in operational condition.
- The new PAMAC platform is **always** up even in case of some of the ROV - UxV connection lost or not in operational condition.
- The new PAMAC platform is able to accept registration on the fly.

5.5.5 Triggers

- one or more ROV - UxV equipped with a Detection Service and a Peripheral Service signal, via sensors, some data (alarm); or
- one or more human query the Base Control System on the same geographic area (low/hot interest); or
- one or more ROV - UxV equipped with a Smart Mobile Application query the Base Control System on the same geographic area (low/hot interest); or
- one or more ROV - UxV loose communication; or
- the new ACT platform infer by the data set a potential interest in a geographical area analyse the ROV - UxV connection lost.

5.5.6 Normal Flow (alarm)

One or more ROV - UxV equipped with a Detection Service and a Peripheral Service are **re-routed** by the Base Control System in another patrolling area, eventually according to a footprint analysis or by data analysis.

5.5.7 Alternative Flow (low/hot interest)

One or more ROV - UxV equipped with a Smart Mobile Application are **re-routed** by the Base Control System in another patrolling area eventually according to a footprint analysis or by data analysis.

5.5.8 Alternative Flow 2

A combination of clauses 5.5.6 and 5.5.7 is possible.

5.5.9 Post-conditions

The patrolling application is responsive and it is able to respond efficiently to their patrolling mission with a fleet that move it dynamically.

5.5.10 High Level Illustration (Normal Flow)

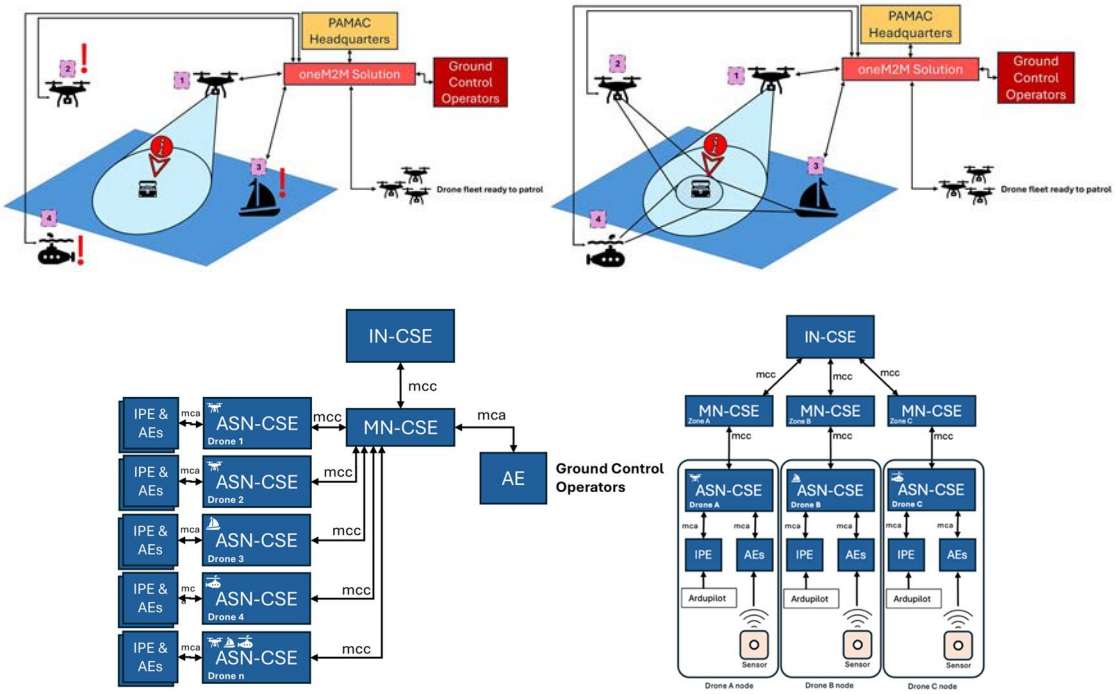

Figure 5.5.10-1: PAMAC Normal Flow

6 Conclusions

The present document contains a list of use cases that cannot be captured by the current version of ACT. These use cases represent an input for evolving the current version of ACT aiming to deploy it within contexts going beyond the COVID-19 scenario, i.e. the scenario inspired the development of ACT.

History

Version	Date	Status
V1.1.1	July 2026	Publication