SocEDA

Cloud based platform for large scale social aware EDA

ANR-10-SEGI-013

Document name:	Requirements of the project
Document version:	0.9
Task code:	T0
Deliverable code:	1.1.1
WP Leader (organisation):	PetalsLink
Deliverable Leader (organisation):	PetalsLink
Authors (organisations):	Pierre CHATEL (THALES)
Date of first version:	01/01/12

Change control

Changes	Author / Entity	Code of version
Creation of the document	Pierre CHATEL / THA	0.1
Outline added	Pierre CHATEL / THA	0.2
Intermediate version	Pierre CHATEL / THA	0.5
New requirements for UC1 – Crisis management; Introduction	Pierre CHATEL / THA	0.9

Acronyms & Abbreviations

ATFM	Air Traffic Flow Management
BC	Binding Component
BPEL	Business Process Execution Language
CDM	Collaborative decision making
CFMU	Central Flow Management Unit (part of Eurocontrol)
EDF	Electricité De France (Operates nuclear plants in France)
ESB	Enterprise Service Bus
FDPS	Flight Data Processing System
FIR	Flight Information Region
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
JBI	Java Business Integration
MEMS	Mobile Emergency Medical Service
POI	Plan d'Opération Interne
PPI	Plan Particulier d'Intervention
RNA	Representative of the National Authority (prefect)
RSN	Radiation Survey Network (measures radioactivity)
SA	Service Assembly
SU	Service Unit
WSDL	Web Semantic Description Language

Table of Contents

1. Introduction

This deliverable deals with the identification and collection of general and technical requirements for the SocEDA platform (see section 3), as well as requirements that are directly linked to the use cases that are going to be developed in the project (see sections 4 and 5). Indeed, while use cases are domain-specific, they are of great help to elicit requirements that have a more global reach to the SocEDA platform as a whole.

This requirement elicitation is structured around a precise methodology that defines a requirements taxonomy and terminology. Both topics are covered by section 2. The taxonomy is used to classify general, technical and use case-related requirements into relevant categories (*functional*, *performance*, *availability*, *accuracy*, *security*, *scalability*, *interoperability*, *awareness & adaptability* and *reliability*) and is used across the document. These categories have been tailored to match the general distributed and event-driven context of SocEDA. Moreover, the requirements terminology, used for the definition of each requirement in the document, helps specify clear and non-ambiguous requirements. The terminology is based on the widely used IETF RFC 2119.

2. Requirements elicitation methodology

A detailed requirements analysis was used to identify the specifications and needed functionality for both Use Cases (see sections 3 and 5) and for the system as a whole (see section 2.2). This requirements specification addresses both **functional** and **non-functional** concerns for the assessment of the solutions developed as part of the project: the Federated Middleware Layer architecture and the monitoring and governance framework.

The requirements process for SocEDA was devised to elicit high level requirements from Use Cases using a scenario-based approach. Using the scenario as a means of requirements elicitation enables the requirements analyst to ground questions in context through the main events described in the scenario. Concerning the second Use Case (Air Traffic Flow Management), Thales analyst consulted internal stakeholders with air traffic flow management domain expertise and accessed Thales documentation to elicit requirements.

2.1. Requirements taxonomy

The requirements were framed using a taxonomy of requirements generally used to improve understanding, analysis and testing of the solution, and are therefore used during requirements elicitation to write clearer more focused requirements. The types, along with example requirements, are presented in the table below.

Requirements Taxonomy		
Functional [FR]:	Something (behavior, function) that a service, stakeholder or system must support.	e.g. a service only supports authenticated consumers
Performance [PR]:	The performance of a service, stakeholder or system enabling a functional requirement.	e.g. desired throughput rates that a service should support
Availability [AvR]:	The minimum required levels of access that stakeholders have on information, services or systems.	e.g. crisis cell field stakeholders high availability
Accuracy [AcR]:	The error rate of a service or system, calculated on the basis of the expected results.	e.g. radiation measurements very high accuracy

Security (& privacy and trust) [SR]:	The minimum levels of security, privacy and/or trust that a service or system should support.	e.g. circle of trust implementation between airport stakeholders
Scalability [ScR]:	The ability of a service or system to process more users' requests, operations or transactions in a given time interval.	e.g. airport services shall be able to deal with huge variation in volume of passengers requests depending on travel exceptions
Interoperability [IR]:	The ability of a service, stakeholder or system to interact with other components or systems.	e.g. support of legacy crisis management information systems
Awareness [AwR] & Adaptability [AdR]:	The level of awareness and predictability that a service, stakeholder or system has over upcoming changes to its specifications or operating environments; as well as its ability to adapt to them.	e.g. media and population situation awareness during the nuclear leak crisis
Reliability [RR]:	The minimum levels of failure that a specific service, stakeholder or system should support.	e.g. a critical airport service shall achieve 99% up-time

2.2. Requirements terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119[1]:

- **MUST**: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
- **SHOULD**: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the

[1] http://www.ietf.org/rfc/rfc2119.txt

full implications must be understood and carefully weighed before choosing a different course.

- **SHOULD NOT**: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY**: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

3. General and Technical Requirements

The "*platform*" term, as used hereafter for simplicity and abstraction reasons in requirements definition, is in fact composed of both the Federated Middleware Layer (WP2) and the Monitoring and Governance Framework (WP3).

ID	Name	Description
Functional		
FR001	Event Driven Architecture Use of events for dynamic information sharing	The platform MUST rely on dynamic events to dispatch and relay information between all interested parties (e.g. service and events consumers and providers).
FR002	Use of "push" paradigm for events routing	The platform MUST rely on the "push" paradigm for information sharing. This paradigm will be implemented by dynamically routing events through the platform.
FR003	Communication of services through events	Any Web service MUST be able to generate events (such as status or UC/business events) that will be sent through the platform.
FR004	Event enrichment	The platform MUST be able to use events routed through it in order to generate new events and enrich the *Event Market Place.*
FR005	Event routing	The platform MUST be able to route events it receives to Web services that are subscribers for that type of events.
FR006	Workflow runtime	The platform MUST provide a JBI-compatible (also based on JSR208 standard) ESB on which to run workflows
FR007	Platform features as Web services	Main features of the platform (e.g., workflow engine, adaptation service, event proxy) SHOULD be deployed in the ESB as Web services and cohabit with external Web services (e.g. services from the UCs).

ID	Name	Description
FR008	Runtime monitoring of workflows	The platform SHALL support the monitoring of workflows at runtime, particularly according to associated nun-functional characteristics.
FR009	Remote surveillance of workflows	Any running workflow MAY be monitored and controlled from remote client position
FR010	Traceability	The platform SHOULD log all service calls and events.
Performance		
PR001	Run of multiple parallel workflows among several web-services	The platform MUST be able to support the runtime of several parallel workflows (representing decisional, operational or support processes in the UCs) among several web-services.
Availability		
AvR001	Web service status update	Any external/partner Web service running on the platform SHOULD update its status (“started”, “work in progress”, “closed”, “error”) when one of its operations is invoked, through events sent to the platform.
Security		
SR001	Confidentiality	Interactions between service and events consumers and providers SHALL be secured to guarantee confidentiality of exchanged sensible data.
SR002	Dynamic access control to services	In case of emergency, services SHOULD have their access control relaxed to authorize temporary consumption.
SR003	Circle of trust	Organizations collaborating within each UC SHALL share user identities or system identities to grant access to their services and data (No central identity management).
SR004	Integrity	Exchanges between organizations SHALL be secured to avoid any corruption of data.

ID	Name	Description
Scalability		
ScR001	Web scale support	The SocEDA platform must be built at Web scale in order to be able combine events from many sources with the goal of connecting and orchestrating services, things and people → the SocEDA platform will revolve around a Cloud architecture.
ScR002	Large Scale workflow support	The number of invoked services in a workflow, as well as exchanged events, varies greatly according to external factors (time of the day, …). As such, the platform MUST have encompassing Large Scale workflows support. This is illustrated by the large list of actors in each SocEDA UC.
ScR003	Highly distributed services support	The services invoked during large scale workflows runtime are highly distributed. The platform MUST support such a context.
ScR004	Service request scalability	The platform MUST be able to deal with variations in number of service requests over time.
ScR005	Events exchange scalability	The platform MUST be able to deal with variations in number of exchanged events over time.
Interoperability		
IR001	Highly heterogeneous services support	The services invoked during large scale workflows runtime are highly heterogeneous (different types). The platform MUST support this heterogeneity by allowing the communication between/to all services.
IR002	Dynamic service discovery	The platform MUST support the dynamic discovery of services at runtime.
IR003	Human interaction	The platform MUST allow for human interaction in the workflows in order to apply modifications at runtime.

ID	Name	Description
IR004	Runtime flexibility	The coordination of all services and events in the system SHALL be highly flexible due to their heterogeneity.
IR005	WS-Notification events support	The platform MUST provide facilities for conversion of WS-Notification events to RDF events (as defined in SocEDA)
IR006	RDF events support	The platform MUST provide facilities for conversion of SocEDA based RDF events to standard WS-Notification events so they can be relayed to events consumers (subscribers).
Awareness & Adaptability		
AdR001	Adaptation of processes and service compositions to current events	The runtime context of processes and service compositions in the platform is linked to current events sent through it. As such, adaption recommendations to these events SHOULD be computed by the platform.
Reliability		
RR001	Message queuing	Exchanges between organisations SHALL be performed in a secured way so that interactions may recover from temporary unavailability of services

4. Requirements from the Crisis Management Use Case (UC1)

The "*Crisis Management System*" (CMS) is the system used in this UC to resolve the crisis. It will be built around the SocEDA platform and its related features. As such, domain requirements over the CMS defined in this section are and/or directly linked to the more general/abstract requirements defined at the general and technical level of the platform (see section 3 for such requirements).

More specifically, as described in deliverable D5.3.1, this CMS is, for the most part, composed of workflows dedicated to crisis management, running on the SocEDA runtime. These workflows are derived from the three classical levels of business processes that exist in any such system: decision, operation and support. This is done to support the agility of both orchestration (internal business processes) and choreography (interactions *between* actors) of the coordination.

ID	Name	Description
Functional		
UC1-FR001	Complex crisis management	The multiplicity and diversity of actors involved in the UC, the volume and heterogeneity of information, the critical dependencies between actions as well as the dynamics of the situation make the crisis management situation particularly complex. The CMS must be built to deal with this complex context.
UC1-FR002	Crisis cell initialization	The CMS MUST implement processes that support crisis cell initialization (Decision level process – as described in D5.3.1).
UC1-FR003	Population protection	The CMS MUST implement processes that support population protection (Decision level process – as described in D5.3.1).
UC1-FR004	Scientific support	The CMS MUST implement processes that support scientific support (Decision level process – as described in D5.3.1).
UC1-FR005	Situation management	The CMS MUST implement processes that support situation management (Decision level process – as described in D5.3.1).

ID	Name	Description
UC1-FR006	Dynamic subscription	The CMS MUST implement processes that support dynamic subscription to events (Decision level process – as described in D5.3.1).
UC1-FR007	Alert and Deploy	The CMS MUST implement processes that support alert and deploy of crisis management stakeholders (Operation level process – as described in D5.3.1).
UC1-FR008	Circulation plan implementation	The CMS MUST implement processes that support circulation plan implementation (Operation level process – as described in D5.3.1).
UC1-FR009	Safety measures implementation	The CMS MUST implement processes that support safety measures implementation (Operation level process – as described in D5.3.1).
UC1-FR010	Victims support	The CMS MUST implement processes that support victim support (Operation level process – as described in D5.3.1).
UC1-FR011	Population evacuation	The CMS MUST implement processes that support population evacuation (Operation level process – as described in D5.3.1).
UC1-FR012	Population confinement	The CMS MUST implement processes that support population confinement (Operation level process – as described in D5.3.1).
UC1-FR013	Iodine distribution	The CMS MUST implement processes that support iodine distribution (Operation level process – as described in D5.3.1).
UC1-FR014	Communication	The CMS MUST implement processes that support communication via media outlets (Operation level process – as described in D5.3.1).

ID	Name	Description
UC1-FR015	Situation assessment	The CMS MUST implement processes that support alert and deploy of crisis management stakeholders (Support level process – as described in D5.3.1).
UC1-FR016	Resources management	The CMS MUST implement processes that support resources management (Support level process – as described in D5.3.1).
UC1-FR017	Data management	The CMS MUST implement processes that support data management (Support level process – as described in D5.3.1).
UC1-FR018	Radiation measurements regular transmission	The radiation survey network (RSN) and Meteo France SHOULD transmit, at regular intervals (every 15 min), their measurements to crisis cell field actors.
UC1-FR019	PPI procedures support	The decision level process for crisis management SHOULD support Global Emergency Plan, or “Plan Particulier d'Intervention” (PPI) in France, procedures.
UC1-FR020	POI procedures support	The decision level process for crisis management SHOULD support Internal Emergency Plan, or “Plan d’Opération Interne” (POI) in France, procedures.
UC1-FR021	Decisions implementation at Operation and Support levels	Operations and Support processes MUST implement the decisions made at the upper crisis management cell level during crisis management.
Performance		
UC1-PR001	National Authority alert delay after leak detection	The representative of the national authority MUST be informed, by the responsible of the nuclear plant, of the nuclear material leakage in less than 1 min after detection.

ID	Name	Description
UC1-PR002	EDF alert delay after leak detection	EDF MUST be informed, by the responsible of the nuclear plant, of the nuclear material leakage in less than 5 min after detection. The National authority then activates the PPI in reflex mode.
UC1-PR003	Crisis cell launch delay	After leakage detection, the crisis cell MUST be launched in less than 15 min by the national authority.
UC1-PR004	Leak detection delay	Leak of the nuclear reactor detection MUST be made, at the power plant level, within 1 sec delay.
Availability		
UC1-AvR001	Crisis cell field stakeholders availability	All crisis cell field stakeholders (firemen, police, army, office of infrastructure, etc.) MUST be available to respond to the crisis ASAP after cell launch.
Accuracy		
UC1-AcR001	Radiation measurements accuracy	RSN and Meteo France SHOULD transmit radiations measurements to field actors with a margin of error bellow 1%.
UC1-AcR002	Crisis-related data transmission accuracy	All crisis-related data transmitted through the CMS SHOULD NOT be deteriorated during transit.
UC1-AcR003	Weather forecasts regular update	To improve accuracy, anticipate any change in wind force and direction or any precipitation, experts from Meteo France SHOULD update weather forecasts at regular intervals (every 30 min).
UC1-AcR004	Safety perimeter accuracy	The crisis cell, based on information received through the CMS, SHOULD define a safety perimeter around the nuclear plant. This safety perimeter (kilometer as base unit) MUST be defined with margin of error bellow 10%.

ID	Name	Description
UC1-AcR005	Circulation plan accuracy	The crisis cell, based on information received through the CMS, SHOULD define a new circulation plan for roads near the nuclear plant in order to ease population evacuation and field stakeholders movements. This safety perimeter (kilometer as base unit) MUST be defined with margin of error bellow 10%.
Security		
UC1-SR001	Experts security advice from IRSN	Institut de Radioprotection et de Sûreté Nucléaire (IRSN) scientific experts SHOULD give their advice on population evacuation, based on measurements received from Meteo France and RSN
Scalability		
UC1-ScR001	High crisis information volume scalability	The CMS MUST be able to deal with high volumes of crisis-related heterogeneous information.
Interoperability		
UC1-IR001	Support of legacy information systems	Crisis management stakeholders can operate with their own (legacy) information system, which may already use web services. The CMS MUST be able to integrate these services.
UC1-IR002	Radiation measurements communication	Despite heterogeneity of legacy Information Systems, RSN and Meteo France MUST be able to transmit their measurements to crisis cell field actors.
UC1-IR002	Multi-level processes interoperability	
Awareness & Adaptability		
UC1-AwR001	Media and population situation awareness	Regular updates SHOULD be given to the media, and then to the population. Every 15 minutes, a new point of the situation SHOULD be provided

ID	Name	Description
UC1-AwR002	Resources status awareness at decision, operation and support levels	The CMS SHOULD be made aware at any time, through events, of the status of stakeholder resources (e.g. thickness of concrete blocks, availability of a specific repairing machine, availability of protection equipments…) at decision, operation and support levels.
UC1-AwR003	Activities status awareness at decision, operation and support levels	The CMS SHOULD be made aware at any time, through events, of the status of stakeholder activities (e.g. radioactivity leak plugging finished, nuclear reactor stopped…) at decision, operation and support levels.
UC1-AwR004	Situational events awareness at decision, operation and support levels	The CMS SHOULD be aware of any notable situational events (e.g. radioactivity limit exceeded at a particular place, consolidated field feedbacks (employees hurt, leak's flow…), absence of wind…) at decision, operation and support levels.
UC1-AwR005	Consequence events awareness at decision, operation and support levels	The CMS SHOULD be aware of any notable consequence events (e.g. explosion in a reactor n°2, e mployee's panic…) at decision, operation and support levels.
UC1-AdR001	Orchestration agility (changes in a single process)	Due to crisis management constraints, the CMS SHOULD provide orchestration runtime agility (reactivity and adaptability), in order to cope with the dynamicity of the context and large number of events that need an immediate response and/or reconfiguration from running orchestrations.

ID	Name	Description
UC1-AdR002	Choreography agility (changes in the interaction between processes)	Due to crisis management constraints, the CMS SHOULD provide choreography runtime agility (reactivity and adaptability), in order to cope with the dynamicity of the context and large number of events that need an immediate response and/or reconfiguration from running choreographies.
Reliability		
UC1-RR001	Data transmission protocols resilience to electromagnetic interferences	Data transmission protocols used by the CMS MUST implement preservation mechanism to prevent data corruption by electromagnetic interferences that could be emitted during the nuclear crisis.
UC1-RR002	Crisis cell distribution	Crisis cell responsibility MUST be distributed between main stakeholders at the local and national levels (e.g. prefects, delegates, national authority, local and/or national experts) in order to improve its reliability and resilience.

5. Requirements from the Air Traffic Flow Management Use Case (UC2)

Air Traffic Flow Management (ATFM) is a service established with the objective of contributing to a safe, orderly and expeditious flow of air traffic by ensuring that air traffic control capacity is utilized to the maximum extent possible, and that the traffic volume is compatible with the capacities declared by the appropriate Air Traffic Services authority.

Moreover, the main objective of ATFM is to optimize the use of the air space to cope with the increasing air traffic, but also, with exceptional situations (such as a crisis over a covered area of responsibility) that may reroute or cancel flights. This is for instance the type of crisis that is described in SocEDA first UC – "Crisis Management".

The "*ATFM system*" term, as used for simplicity reasons in this UC, is an abstraction of the Air Traffic Flow Management responsibility that is distributed between ATC centers and the CFMU (Central Flow Management Unit[2] - part of Eurocontrol) in Europe.

Air Traffic Control (ATC), as part of the more global ATFM service, is a service provided by ground-based controllers who direct aircraft on the ground and in the air. This to separate, organize and expedite the flow of air traffic, but at the local Flight Information Region (FIR) level.

ID	Name	Description
Functional		
UC2-FR001	Computation of planes routes by ATFM system	Based on air traffic and airports congestion, as well as weather conditions, the ATFM system MUST be able to provide alternate routes to planes in order to safely reach their final destination in due time. This translates to rerouting request sent to impacted parties (e.g. pilots, ATCs, airports, CFMU, …) as detailed in other requirements.
UC2-FR002	External communication	The ATFM system MAY provide up-to-date air traffic information via different media (e.g. regular website updates, real-time twitter posts and responses)

[2] http://www.cfmu.eurocontrol.int

ID	Name	Description
Performance		
UC2-PR001	Onboard flight status updates	Passengers SHALL be informed of any changes to their flight status within 5 minutes of the information being available
UC2-PR002	Collaborative ATFM decision making (CDM)	The Airport Authorities, ATC centers, Airlines and CFMU SHALL be provided with services to support collaborative ATFM decision making.
UC2-PR003	ATFM CDM information propagation times	The Airport Authority, ATC, Airline and Ground Handlers SHALL be provided with real-time information sharing (e.g. information propagation time to all actors in less than 10 seconds)
UC2-PR004	Reroute request delay	A pilot MUST be made aware of a reroute request from the ATC of the Flight Information Region (FIR) he is located in, in less than 5 seconds.
UC2-PR005	Delay to inform all impacted planes of ATFM decisions	All planes impacted by an ATFM flow regulation decision (in flight or on the ground before takeoff), such as a reroute requests, MUST be informed in less than 5 minutes.
UC2-PR006	Delay to close runways in case of bad weather	After decision has been made by local airport authorities to close runways due to bad weather, all airport runways SHOULD be closed in less than 30 minutes and information propagated through the ATFM system to all concerned actors in the meantime.
UC2-PR007	Reroute agreement delay	In case of flight plan modification, agreement on final destination between the pilot and ATC SHALL take less than 10 minutes

ID	Name	Description
UC2-PR008	Flight plan modification agreement broadcasting delay	In case of flight plan modification, agreement on final destination SHALL be transferred by ground-based controller (ATC) to impacted parties (airline operating the flight, CFMU, alternate destination airport, etc.) in less than 3 minutes.
Availability		
UC2-AvR001	Flight plan access by ground-based controllers	Any ground-based controller SHALL be able to access at all time the detailed flight plan for each flight in its FIR: this concerns flights going to or departing from its airport, in Taxi, as well as flights currently en route in its FIR.
UC2-AvR002	Alternate airport list availability	A pilot MUST be able to access the pre-computed list of alternate airports at his disposal at any time during its flight
UC2-AvR003	Aiports congestion status availability	Current airports congestion status SHALL be updated on the fly and made available to the ATFM system.
Accuracy		
UC2-AcR001	Rerouted plane arrival time accuracy	When a plane needs to be rerouted following an ATFM regulation decision, the new time of arrival, as propagated to impacted parties, SHALL be accurate to the minute.
Security		
UC2-SR001	Dynamic access control to passenger data	Due to ATFM constraints, access to travel data SHALL be granted to applications/operators in exceptional situations (e.g. crisis that impact flight plans). Modification of access rights, if any, SHALL be temporary and attached to the context.

ID	Name	Description
UC2-SR002	Dynamic access control to static environment data	Due to ATFM constraints, access to environment data (static data which describes air space and airport) MUST be granted to applications/operators according to circumstances. Modification of access rights, if any, SHALL be temporary and attached to the context.
Scalability		
UC2-ScR001	Air Traffic Flow Management punctual scalability	The ATFM system MUST be able to deal with seasonal variations of flights numbers (e.g. during vacation times, or specific events like World Cups).
UC2-ScR002	Air Traffic Flow Management daily scalability	The ATFM system MUST be able to deal with the daily flightboards and related dynamic events from its airports, planes and ATC centers.
UC2-ScR003	Plane rerouting scalability	The ATFM system MUST be able to deal with significant variations in the number of planes that need to be notified (depending on the day, time, period of the year, exceptional events, etc.).
Interoperability		
UC2-IR001	Communication channels interoperability	Parties impacted by ATFM regulation SHALL be able to communicate with each other, and dynamic events exchanged, even if they rely on heterogeneous (legacy) communication channels.
Awareness & Adaptability		
UC2-AdR001	Adaptation to traffic congestion (related to UC2-FR001)	The ATFM system MUST adapt to current air traffic congestion) in the flying areas it manages.
UC2-AdR002	Adaptation to weather conditions (related to UC2-FR001)	The ATFM system MUST adapt to current weather(s) in the flying areas it manages.

ID	Name	Description
UC2-AdR003	Adaptation to airports congestion (related to UC2-FR001)	The ATFM system MUST adapt to current airports congestion status in the areas it manages.
UC2-AdR004	Adaptation to ATFM indirect consequences: rescheduled passengers	Passengers that were not originally scheduled for a given flight, but that need to be rescheduled (due to ATFM regulation) SHALL be dealt with.
UC2-AwR001	Traffic congestion status awareness	The ATFM system SHALL be aware at all time of current air traffic congestion) in the flying areas it manages.
UC2-AwR002	ATC weather awareness	ATCs part of the ATFM system MUST be aware at all time of current weather conditions for planes in their managed FIRs (i.e. 24/7 access to weather forecast service).
UC2-AwR003	Airports congestion status awareness	The ATFM system SHALL be aware at all time of current airports congestion status in the areas it manages.
Reliability		
UC2-RR001	Communication channels reliability	Critical communication channels used for communication and events exchange between the pilot and ATC MUST achieve 99% up-time.