SYnergy of integrated Sensors and Technologies for urban sEcured environMent

D7.1
Report on requirements for HW and SW

3 September 2019 **V3.0**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787128

Project title	SYnergy of integrated Sensors and Technologies for urban sEcured environment
Project acronym	SYSTEM
Project number	787128
Start date of the project	1st September, 2018
Duration	36 months
Topic	SEC-10-FCT-2017. Integration of detection capabilities and data fusion with utility providers' network

Deliverable number	D7.1
Deliverable title	Report on requirements for HW and SW
Leading partner	RESI
Partners contributing	RESI
WP of reference	WP7
Title of the WP of reference	DATA AND INFORMATION FUSION
Task of reference	T7.1
Title of the task of reference	Software design and integration: finalization of requirements for Hardware and Software
Deliverable type	Report
Dissemination level	PUBLIC
Due date	M11 – July 2019

Keywords	Data fusion, software integration, data collection
Abstract	The purpose of this document is to report on the activities conducted and choices made in order to configure, customize and deploy the GENESI® Monitoring Centre to integrate data sent by SYSTEM sensors and elaborate them with a data fusion engine to be implemented as an extension of the Monitoring Centre. This document goes through the hardware and software requirements specification, followed by the explanation of the rationale followed to produce a customized version of the Monitoring Centre.

Editor	Manuel Mastrofini (RESI) Pietro Guerrieri (RESI)
Contributors	Manuel Mastrofini [RESI] Pietro Guerrieri [RESI]
Reviewers	Krause, Steffen (UNI BWM) Pötter, Harald (Fraunhofer)
Submission date of the draft to reviewers	10/07/2019

Submission date of the draft to the SAB (if required)	Not required

Register of document versions

Partner acronym	Version number	Date	Suggested relevant changes	Notes
RESI	V1.0	10/7/2019		First version ready for review
UNI BWM	V2.0	15/07/2019	The terminology for device, sensor, subsystem should be the same as in D1.1.	Some entries in the list of acronyms are missing (s. comments) For multiple elements of the FEAT_ list an explanation is missing.
Fraunhofer	V2.1	24/07/2019	Some comments	
RESI	V2.2	28/07/2019		Integration of V2.1 and V2.2 revisions. Minor changes to wording and sentence structure.
FORMIT	V3.0	02/09/2019	None	

Every information is updated to the date of issue of this document

This document is composed by 27 pages

Table of Contents

List of acronyms and abbreviations

API	Application Programming Interface
CA	Consortium Agreement
CoAP	Constrained Application Protocol
COTS	Commercial Off The Shelf
CRUD	Create/Read/Update/Delete
DoA	Description of Action
EB	Executive Board
EC	European Commission *or* Electrical Conductivity
ES	Exploitation Strategy
GA	Grant Agreement
GDPR	Global Data Protection Regulation
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
MC	Monitoring Centre
RBAC	Role-Based Access Control
REST	Representational State Transfer
RDBMS	Relational Database Management System
SAN	Storage Area Network
SME	Small and Medium Enterprise
UAC	User Access Control

EXECUTIVE SUMMARY

The purpose of this document is to report on the activities conducted and choices made in order to configure, customize and deploy the GENESI® Monitoring Centre to integrate data sent by SYSTEM sensors and elaborate them with a data fusion engine to be implemented as an extension of the Monitoring Centre (MC).
This document goes through the hardware and software requirements specification, followed by the explanation of the rationale followed to produce a customized version of the Monitoring Centre.

The Monitoring Centre is a centralized server collecting sensors data via secured communication channels and offering APIs to access and elaborate the stored data. Data can be accessed according to a fully configurable set of privileges. Access undergoes a strict tracking policy and the Monitoring Centre assures that data cannot be altered nor accessed without leaving traces in the system. Furthermore, the Monitoring Centre ensures data integrity and non-repudiability. Finally, the Monitoring Centre offers API for adding devices, preparing missions and configuring access policies or system parameters.

The Monitoring Centre also includes a component to display information to the LEA and utility network operators, according to customized access rights. This component is named Control Station. It consists in mobile devices, desktop computers or laptop computers running a client-side application, which receives data from the Monitoring Centre and allows to visualize and explore data.
The client side application can be a native application (e.g. an App for Android devices) or a web application.

This document reports the requirements specification and preliminary design, by providing software and hardware requirements specifications and some architectural decision rationales.

1 MAIN ELEMENTS OF THIS DELIVERABLE

1.1 INPUT FROM OTHER PROJECTS

Excerpts of the preliminary design and executive design of the NOSY project are reused and reworked in this document, specifically, data model and wireframes.

1.2 INPUT FROM OTHER WPS AND RELATION WITH OTHER SYSTEM DELIVERABLES

The main inputs to this document are D1.1 (*Requirements, scenario definition and system concept*) and D1.2 (*Data retrieval definition*).

1.3 APPLICABILITY

The deliverable *Report on requirements for HW and SW* (D7.1) aims at becoming the reference point to configure, customize and deploy the GENESI® Monitoring Centre in order to integrate data sent by SYSTEM sensors and elaborate them with a data fusion engine.

1.4 REFERENCE DOCUMENTS

In order to set a framework in matter of a conflict between the Project Operational and Management Plan (D12.1) and other documents such as the Description of Actions (DoA) or the Grant Agreement, the following hierarchy will be applied:

1. Grant Agreement (GA) (and its amendments);
2. Consortium Agreement (CA);
3. The Project Operational and Management Plan (D12.1).

The hierarchy related to the documents above implies that the latter document needs to be consistent with the former. In case of issues, this hierarchy of documents is mandatory.

1.5 PURPOSE OF THE DOCUMENT

The purpose of this document is to report on the activities conducted and choices made in order to configure, customize and deploy the GENESI® Monitoring Centre to integrate data sent by SYSTEM sensors and elaborate them with a data fusion engine to be implemented as an extension of the Monitoring Centre.
This document goes through the hardware and software requirements specification, followed by the explanation of the rationale followed to produce a customized version of the Monitoring Centre.

1.6 STRUCTURE OF THE DOCUMENT

The document is structured in the following way:

1. **Main elements of this deliverable:** this introduction
2. **Software Requirements**: high-level specification of software requirements
3. **Software Architecture and Rationales**: architectural decisions undertaken and their explanations
4. **Software Technical Features**: low-level specification of software requirements
5. **Hardware requirements**: specification of hardware components and their usage

1.7 ADOPTED CONVENTIONS

The notation used to identify the different requirements is the following:

- For software requirements: [TYPE_LABEL_XXXX], where:
  - TYPE: indicates the type of the requirement, i.e.:

        - SWREQ: it is a user requirement;
        - FEAT: it is a software feature
    - LABEL: an optional mnemonic label to give a hint on the requirement content
    - XXXX: a 4-digit number to uniquely identify the requirement.

This document follows the taxonomy below for requirements, according to IETF RFC2119:

- SHALL – This word, or the terms "REQUIRED" or "MUST", means that the definition is an absolute requirement of the specification.
- SHALL NOT – This phrase, or the phrase "MUST NOT", means that the definition is an absolute prohibition of the specification.
- SHOULD – This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT – This phrase, or the phrase "NOT RECOMMENDED", means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY – This word, or the adjective "OPTIONAL," means that an item is truly discretionary.

2 SOFTWARE REQUIREMENTS

2.1 REQUIREMENTS SPECIFICATION

ID	SWREQ_RBAC_0001
Name	User Management
General Description	The Monitoring Centre shall allow user CRUD. Each user has first name, last name, email address, telephone number, additional notes, a personal picture and a belonging organization (LEA or Utility Network or partner). Each user is assigned a unique username (user id). The system shall create the first user to access the system with default credentials.

ID	SWREQ_RBAC_0002
Name	Password Management
General Description	On user creation, a temporary password is generated, which shall be updated at first login. The password shall be subject to expiration and renewal. Password shall be at least 8 characters and include at least one uppercase character, one lowercase character and one non-letter character.

ID	SWREQ_RBAC_0003
Name	Role Management
General Description	The Monitoring Centre shall allow role CRUD. Each user is assigned one or more roles. The Monitoring Centre shall allow to attribute a specific privilege, taken from a predefined set of privileges, to a role or to a single user. The Monitoring Centre shall allow a user to perform operations only according to the granted privileges.

ID	SWREQ_RBAC_0004
Name	Access traceability
General Description	Access to measurement data shall be allowed only if appropriate privileges exist and every access or operation performed shall be recorded.

ID	SWREQ_RBAC_0005
Name	Access report
General Description	The Monitoring Centre shall allow to visualize the list of operations recorded for a single user and the list of operations performed on a given measurement, including create timestamp and list of recorded accesses.

ID	SWREQ_DEVICE_0001
Name	Device Management
General Description	The Monitoring Centre shall allow to configure the list of devices enabled to connect and communicate with the Monitoring Centre. Devices are characterized in terms of: name, typology, id or serial number, device version, software version, firmware version, operation area, assignee (a user), additional notes.

ID	SWREQ_DEVICE_0002
Name	Device Reconfiguration
General Description	The Monitoring Centre shall allow to set some device configurations, according to reconfiguration functions supported by each device.

ID	SWREQ_SYNC_0001

Name	Clock Synchronization
General Description	The Monitoring Centre and the Control Station should synchronize with respect to a reference clock, namely the Master Clock.

ID	SWREQ_PRIVACY_0001
Name	Privacy compliance
General Description	The Monitoring Centre and Control Station should be compliant with the privacy regulations for storing sensitive data, including GDPR

ID	SWREQ_DIAGNOSIS_0001
Name	Field Device status
General Description	The Monitoring Centre shall be able to retrieve information concerning the status (e.g. operational capability, integrity and position) of sensors.

ID	SWREQ_DIAGNOSIS_0002
Name	Field Device expert mode
General Description	The Monitoring Centre should be able to show low-level details (e.g. real-time data stream or debug data) coming from each device.

ID	SWREQ_DIAGNOSIS_0003
Name	Field Device calibration mode
General Description	The Monitoring Centre should be able to issue calibration commands to each device that support remote calibration.

ID	SWREQ_MEASUREMENT_0001
Name	Alarms and measurements management
General Description	The Monitoring Centre shall receive and store alarms and measurements from the Field Devices to the Monitoring Centre.

ID	SWREQ_MEASUREMENT_0002

Name	Alarms and measurements data storage
General Description	The Monitoring Centre shall store the data for each measurement or alarm according to the data integration reported in D1.2

ID	SWREQ_MEASUREMENT_0003
Name	Measurement collection
General Description	The Monitoring Centre shall be able to gather data coming from the sensors, including the cases where the communication is mediated by other devices.

ID	SWREQ_MEASUREMENT_0004
Name	Measurement and Alarm data API
General Description	The Monitoring Centre shall expose APIs to allow the Control Station to access stored data, according to privileges granted to the user requiring the data.

ID	SWREQ_MEASUREMENT_0005
Name	Mission Management
General Description	The Monitoring Centre shall support CRUD for missions and shall associate data collected to a mission. Each mission has a unique identifier generated by the Monitoring Centre and is characterized by: ● start and end dates ● involved locations ● involved organizations ● substances of interest ● used devices and corresponding investigator, if any ● set of keys for encryption and decryption ● set of setups and configurations for each device ● area of interest Changes to a mission shall be recorded.

ID	SWREQ_MEASUREMENT_0006
Name	Alarm notifications
General Description	The Monitoring Centre should notify the appropriate users when

	relevant information is acquired.

ID	SWREQ_MEASUREMENT_0007
Name	Real time data
General Description	The Monitoring Centre shall send data to a Control Station that registered a set of filtering criteria for real-time communication

ID	SWREQ_MEASUREMENT_0008
Name	Data fusion scaffold
General Description	The Monitoring Centre shall provide a flexible scaffold of a data fusion engine to be extended over project time

ID	SWREQ_MEASUREMENT_0009
Name	Mathematical/Probabilistic model support
General Description	The Monitoring Centre shall be designed to support the implementation of mathematical/probabilistic models to integrate in the data fusion engine, in order to support the identification of events of interest

ID	SWREQ_MEASUREMENT_0010
Name	Pattern recognition support
General Description	The Monitoring Centre shall be designed to support the implementation of pattern recognition algorithms to integrate in the data fusion engine, in order to support the identification of events of interest

ID	SWREQ_MEASUREMENT_0011
Name	Fluid dynamic model support
General Description	The Monitoring Centre should be designed to support the implementation of fluid dynamic model to integrate results from a hydraulic model in the data fusion engine, in order to support the identification of a substance discharge location

ID	SWREQ_MEASUREMENT_0012
Name	Basic artificial intelligence support
General Description	The Monitoring Centre may be designed to support the implementation of a basic artificial intelligence function to integrate in the data fusion engine

ID	SWREQ_MEASUREMENT_0013
Name	Basic machine learning support
General Description	The Monitoring Centre may be designed to support the implementation of a basic machine learning function to integrate in the data fusion engine

ID	SWREQ_MEASUREMENT_0014
Name	Custom data fusion logic
General Description	The Monitoring Centre should support the implementation of custom logic as an extension of the data fusion engine, in order to improve the data fusion performance

ID	SWREQ_MEASUREMENT_0015
Name	Data fusion recommendation
General Description	The Monitoring Centre should produce recommendations for the operators by leveraging the results of the data fusion engine

ID	SWREQ_ANALYSIS_0001
Name	Data search
General Description	The Monitoring Centre shall allow a user to search through data by predefined criteria: ● Sensor type ● date range ● Substance ● Location ● Full text ● Mission Results shall be shown according to user's privileges.

ID	SWREQ_ANALYSIS_0002
Name	Reporting
General Description	The Monitoring Centre should allow a user to create reports with filtered data via Control Station.

ID	SWREQ_ANALYSIS_0003
Name	Data export
General Description	The Monitoring Centre shall allow a user to export a report via Control Station by selecting from a preconfigured set of report templates.

ID	SWREQ_ANALYSIS_0004
Name	Data import
General Description	The Monitoring Centre shall allow a user to import via Control Station and visualize data coming from external systems and containing sensors information and collected measurements.

ID	SWREQ_ANALYSIS_0005
Name	Geographic Data import
General Description	The Monitoring Centre should support the integration of geographic data to enrich the data collected by sensors.

ID	SWREQ_SECURITY_0001
Name	Identity
General Description	The Monitoring Centre and Control Station shall ensure identity of sender both for data exchange and configuration purposes via digital signature.

ID	SWREQ_SECURITY_0002
Name	Minimum-privilege

General Description	The Monitoring Centre shall provide a mechanism to implement the "Minimum-privilege" principle.

ID	SWREQ_SECURITY_0003
Name	Segregation of duties
General Description	The Monitoring Centre shall provide a mechanism to implement the "Segregation of duties" principle.

ID	SWREQ_SECURITY_0004
Name	Layered-security and Defense-in-depth
General Description	The Monitoring Centre and the repository shall be designed according to the "Layered-security" and "Defense-in-depth" principle.

ID	SWREQ_SECURITY_0005
Name	Encryption and Integrity
General Description	The Monitoring Centre and Control Station shall encrypt and decrypt data exchanged and ensure data integrity.

ID	SWREQ_SECURITY_0006
Name	Digital hash on communication channels
General Description	The Monitoring Centre and Control Station shall verify data integrity via digital hash in all communications.

ID	SWREQ_SECURITY_0007
Name	Digital hash on repository
General Description	The Monitoring Centre shall verify data integrity via digital hash when reading from and writing to the repository.

ID	SWREQ_SECURITY_0008
Name	Encrypted repository
General Description	The Monitoring Centre shall store only encrypted data.

ID	SWREQ_SECURITY_0008
Name	Secured communication channels
General Description	The Monitoring Centre and Control stations should communicate over a Virtual Private Network, when supported by a sensor

ID	SWREQ_AVAILABILITY_0001
Name	Availability
General Description	The Monitoring Centre should guarantee the availability of the data stored in the Data Centre.

3 SOFTWARE ARCHITECTURE AND RATIONALES

Many of the requirements specified in the previous section are shared between SYSTEM and NOSY. As a consequence, most decisions concerning SYSTEM preliminary design for the Monitoring Centre follow the steps already made in NOSY. Also, the GENESI® MC (i.e. the product that RESI owns) is already in production for many customers to support audio/video data streaming and gps-tracking centered on human targets.

Some additional functions specific to the NOSY project were already developed for that project. In particular, in NOSY, as well as in SYSTEM, most of the features offered by GENESI can be reused and easily adapted to manage a different type of data, i.e. measurements coming from the NOSY and MicroMole devices.

Nevertheless, according to the previously specified requirements, the way in which GENESI is expected to be used for SYSTEM is different from its standard employ, but it is similar to what NOSY required. In fact, NOSY, as well as SYSTEM, requires a mission-centric approach for the Monitoring Centre: no one human target was the focus of the monitoring activity. The focus of the system is a mission, i.e. a time-bounded interval in which a set of devices is deployed to several locations to detect illicit substances or laboratories. In each mission, different LEA or utility network personnel can be employed and different configurations can be set up for each system component.

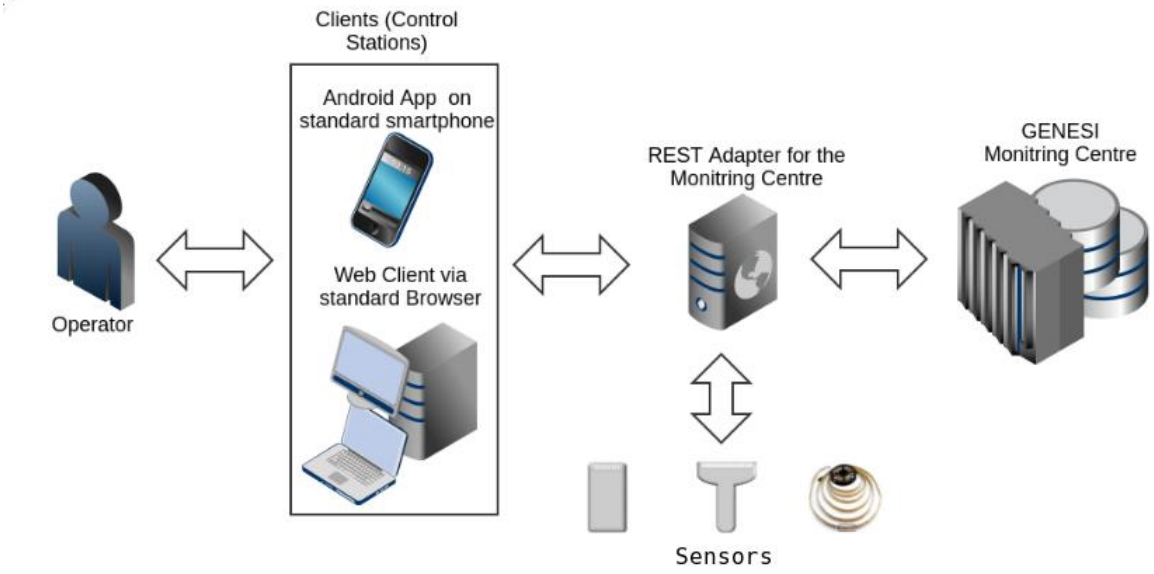
Because of this, the decision taken for the deployment of the GENESI® MC in SYSTEM can be synthesized in the following points:

- A new Control Station will be developed for the SYSTEM project, leveraging and augmenting what already was developed in NOSY.
- The back-end functionalities already in place into the Monitoring Centre (which include data management, data collection, data security, data elaboration and role-based access control) can be completely reused without the need for new implementation, but only adaption and configuration for SYSTEM specific needs.
- The adapter between Control Station and Monitoring Centre will be extended to support the new sources of data, the new formats and the new protocols supported by the sensors employed in SYSTEM.

In terms of technology:

- The Web Client Application is developed using mainly Angular 1.4 and Bootstrap 3, along with many of their add-ons
- The Android Client App is developed using Cordova
- The set of APIs exposing the pre-existing Monitoring Centre functionalities is developed in Java 8, Spring Framework and Hibernate, and follows a standard REST architecture
- Data exchanged between clients and Monitoring Centre, as well as between Field Devices and Monitoring Centre via Handheld Controller, are in JSON format and use HTTP as transport protocol.

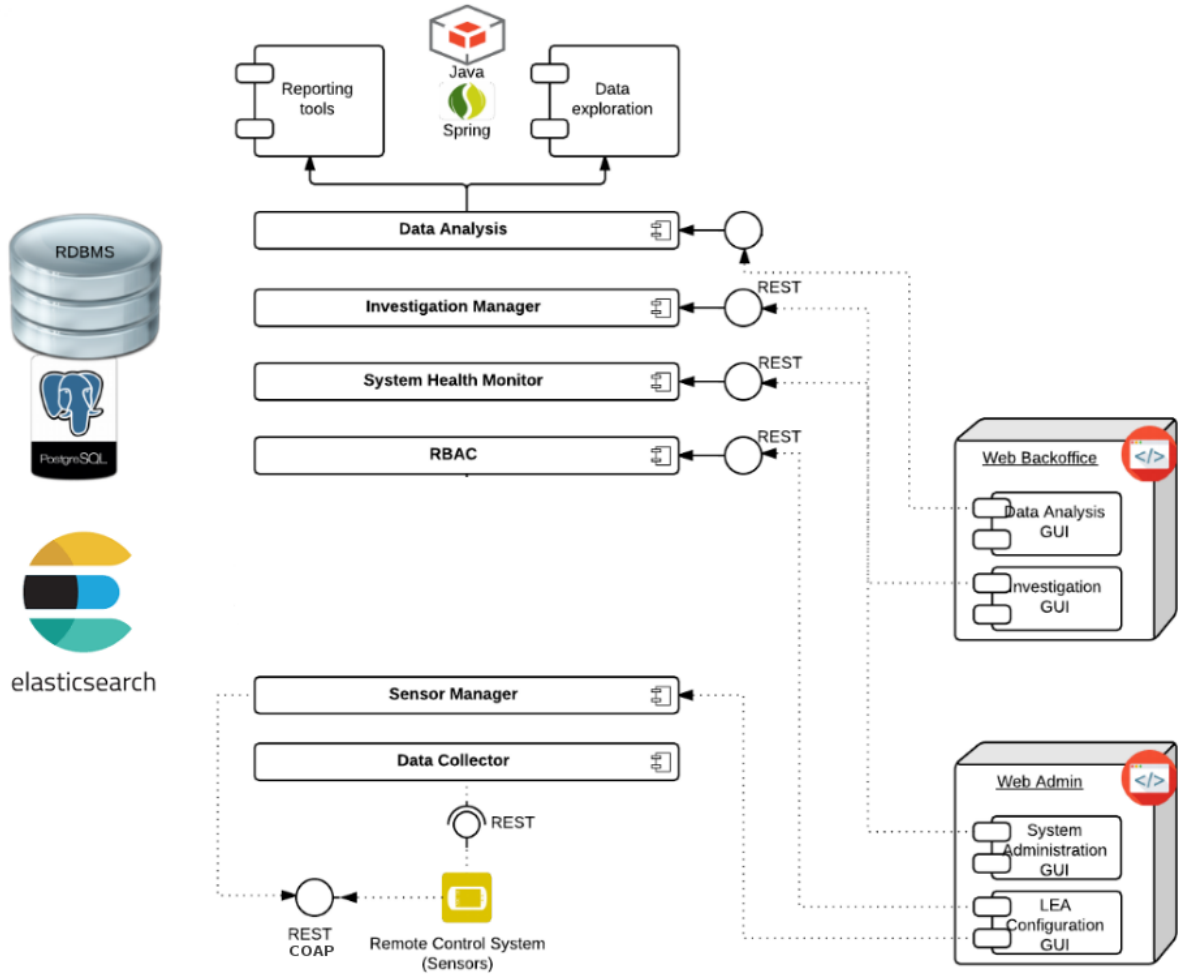
The following image shows how Monitoring Centre, its REST adapter, and the Control Stations interact with the other system components.



3.1 SOFTWARE LOGICAL COMPONENTS

According to the previously specified requirements, some components can be identified for implementation (or reuse and configuration, in case they already exist in GENESI® MC or in the Control Station developed for NOSY). The logical components identified are:

- Data analysis: it implements the data fusion engine and allows to search and explore data, to produce reports and to export data
- Investigation manager: it implements the functions to support mission management
- System health check manager: it implements the features to monitor the status of sensors attached to the Monitoring Centre, and to notify the appropriate operators on that
- RBAC (Role-Based Access Control): it implements the functions to configure the application privileges, access rights and users.
- Sensor manager: it implements the functions to attach and manage the sensors deployed in SYSTEM and present their configuration to the operators
- Data collector: it implements the API (REST and COAP) to receive the data coming from sensors deployed in SYSTEM
- Web admin and Web back office: client applications to allow the operators to interact with the system
- RDBMS (PostgreSQL) and Elasticsearch: software components that allow to store and elaborate the measurements



4 SOFTWARE TECHNICAL FEATURES

4.1 MONITORING CENTRE

The features in the following table relates to the Monitoring Centre and are sorted by source use case. GUIs for Control Stations, both Web and Android, are dealt with separately and are not included in the following table.

Technical features reported in this document are created from what defined for the NOSY project, on top of which the missing features are added and existing features are slightly adapted to comply with the new requirements.

ID	Name	Details
FEAT_0011	Issue configuration command	Configure a device in terms of: operating mode, duty cycle, substance quantity alarm threshold, data transmission policy, battery usage policy, and data storage policy.
FEAT_0012	Import configuration file for mission	Devices employed for a mission and deployed keys shall be imported into the system by the mission head. The configuration cannot be changed manually, but only via verified file import. The structure of the file to import is defined separately.

FEAT_0024	Manage keys	The system shall store keys used for data encryption and identification in order to use them to decrypt and validate received data.
FEAT_0097	Setup devices per mission	During configuration import, devices need to get associated to a mission, so that they become part of the field device deployment layout for that mission. Device data: name, typology, id or serial number, software version, firmware version, operation area, assignee (a user), additional notes and sensors on board.
FEAT_0099	Log configuration import	Register all import operations
FEAT_0101	Log key changes	Register all changes to authorization keys
FEAT_0125	Perform mission devices health check	Operational capability, integrity and possible further information related to devices deployed for a mission.
FEAT_0126	Perform devices health check	Operational capability, integrity and possible further information related to devices for which the organization of the current user is responsible.
FEAT_0127	Perform devices debug	Low-level information coming from the device.
FEAT_0043	Log query executed for data retrieval	Register all queries executed to retrieve data
FEAT_0044	Filter data by date range	
FEAT_0045	Filter data by mission	
FEAT_0046	Filter data by device type	
FEAT_0047	Filter data by specific device	
FEAT_0048	Apply multiple filtering criteria	
FEAT_0062	Filter data by level of alarm	
FEAT_0133	Filter data by substance category	
FEAT_0168	Filter data by substance	
FEAT_0134	Filter data by location	
FEAT_0135	Filter by full-text search	Search any text in all measurement data.

FEAT_0025	CRUD mission	Store: start and end dates involved locations involved organizations substances of interest used devices, devices registered for real-time notifications, and corresponding investigator, if any notification configuration (enabled/disabled, receivers) and keys
FEAT_0026	Associate mission to devices configuration	When importing a configuration it shall be associated to a mission
FEAT_0103	Log attach/detach device to mission	Register all device attach/detach operations
FEAT_0146	Retrieve mission configuration details	List devices, sensors, measurements and alarms for a mission
FEAT_0147	List mission within LEA	
FEAT_0015	CRUD roles	Roles have one of the following scopes: ● System: the role is accessible from all operators and associated privileges apply system-wide. ● Organization-specific: the role is associated to an organization and associated privileges apply to that organization only. ● Mission-specific: the role is associated to an operator and associated privileges apply to that mission only. The following standard roles exist: ● One system role for "system administrator". ● Two organization-specific roles: "Organization managing personnel" and "Organization non-managing personnel". ● Two Mission-specific roles: "mission head" and "mission operator". Standard roles cannot be edited or deleted. Additional roles can be created, edited, viewed and deleted.
FEAT_0016	CRUD users	
FEAT_0018	Role-based matrix for UAC	Manage a matrix whose rows are roles and columns are functions (pre-defined privileges) enabled for that role.
FEAT_0019	User-based matrix for UAC	Manage a matrix whose rows are users and columns are functions (pre-defined privileges) enabled for that user. User-level configurations override role-level configurations.
FEAT_0020	User Authentication	
FEAT_0021	User Authorization according to RBAC matrices	When requiring access to a function and/or to data, a user is authorized according to user-privileges and role-privileges matrices.
FEAT_0022	Device Authorization & Authentication	When receiving data from a device, the sender shall be authenticated and authorized to transmit data to for a mission by checking the imported configuration.

FEAT_0035	Log user access	
FEAT_0036	Log user creation	
FEAT_0037	Log user change	
FEAT_0038	Log user removal	
FEAT_0039	Log UAC change	
FEAT_0040	Log user authorization	
FEAT_0080	Assign role to user	System administrators and organization managing personnel can assign the organization managing personnel role to a user. Organization managing personnel can assign organization non-managing personnel role to a user. Organization managing personnel having the Mission head role for a specific mission can assign the Mission operator role to a user for that mission. Organization managing personnel having the Mission head role for a specific mission can assign the Mission head role to a user for that mission.
FEAT_0081	Assign privileges (pre-defined) to role	Each role can be assigned diverse privileges, chosen by a predefined set of privileges. The set of privileges is defined separately. System administrators can edit privileges standard role. Organization Managing personnel can edit privileges for additional roles.
FEAT_0082	Assign privileges (pre-defined) to user	Each user can be assigned diverse privileges, chosen by a predefined set of privileges. The set of privileges is defined separately. Organization managing personnel can assign privileges to specific users.
FEAT_0169	CRUD Organizations	Name, address, nature (LEA, Utility Network)
FEAT_0149	Manage password	Generate one-time-use passwords for new user accounts. Force renewal of password at expiration, which happens after a configurable number of days since last update (default 60). Validate password: it shall be at least 8 characters and include at least one uppercase character, one lowercase character and one non-letter character.
FEAT_0150	Password expiration	Force expired password change at login
FEAT_0027	Receive Data from devices	Listen to devices sending data.
FEAT_0028	Decrypt and accept data received from devices	Verify the sender's identity, verify data integrity.

FEAT_0029	Store device data with digest	Digest shall ensure data integrity.
FEAT_0030	Store data received with encryption	Data received shall be encrypted before storage.
FEAT_0031	Log recent discarded data	
FEAT_0032	Log data stored	
FEAT_0033	Log command issued	
FEAT_0041	Log device access	
FEAT_0042	Log device authorization	
FEAT_0123	Generate notifications on alarm	If notifications are enabled for a mission, one shall be generated when receiving an alarm and sent to involved users via email.
FEAT_0065	Compute metrics on filtered data	Total of alarms. Alarms to measurement ratio. Average time between two alarms. Alarm break down by substance. Alarm break down by mission. Alarm break down by device type. Alarm break down by device. Alarm break down by location.
FEAT_0098	Log metrics computed	
FEAT_0105	Configure reports	Configure which data to include and the level of detail of the report to export. The level of detail allows to set whether to include all types of measurements or alarms only, whether to show measurement details, or whether to show device details.
FEAT_0106	List report templates	
FEAT_0128	Produce reports on demand	
FEAT_0129	Automatically send reports	Report configuration is set in mission CRUD.
FEAT_0130	Log report creation	
FEAT_0131	Log report configuration	
FEAT_0132	Fetch predefined report templates	Built-in templates are loaded into the system during initialization.
FEAT_0013	Setup Monitoring Centre basic configuration	Set all configurable variables of the system.

FEAT_0014	Create syadmin user	Initial credentials for first automatically generated user: sysadmin/NOSYNOSY000 Personal information: first name, last name, email address, 3 telephone numbers, additional notes, a personal picture and a belonging organization
FEAT_0100	Log basic MC configuration change	
FEAT_0107	Setup regular report generation	Configure report templates.
FEAT_0140	Configure email notification template	Setup the email template to send when an alarm is triggered
FEAT_0120	Show changes to users and roles	List all changes occurred to users and roles.
FEAT_0153	Fetch data for mission	Load a text file containing measurement data collected by devices not attached to the Monitoring Centre, but related to a mission
FEAT_0157	CRUD for devices and real-time filtering criteria	Register an authorized device to receive real-time notification according to some filtering criteria (mandatory time range)
FEAT_0158	Notify registered devices real-time	Send a notification to all devices registered to receive real-time information
FEAT_0171	Data fusion scaffold	There exists a set of technical guidelines to follow in order to implement extensions to the core of the data fusion engine
FEAT_0172	Mathematical model support	The data fusion engine supports the extension with mathematical models which produce as an output the probability that an event of interest happened in a specific are and within a specific time window
FEAT_0173	Probabilistic model support	The data fusion engine supports the extension with probabilistic models which produce as an output the probability that an event of interest happened in a specific are and within a specific time window
FEAT_0174	Pattern recognition support	The data fusion engine supports the implementation and configuration of a repository with reference pattern against which the collected data are compared
FEAT_0175	Pattern recognition support	The data fusion engine supports the extension with a pattern matching algorithm to compare the collected data against the reference patterns configured into the system, in order to provide a probability that an event of interest happened
FEAT_0177	Fluid dynamic model support	The data fusion engine supports the extension with fluid dynamic models to integrate in the data fusion engine, in order

		to support the identification of a substance discharge location
FEAT_0178	Basic artificial intelligence support	The data fusion engine defines some guidelines to support and possibly implement some form of artificial intelligence
FEAT_0179	Basic machine learning support	The data fusion engine defines some guidelines to support and possibly implement some form of machine learning
FEAT_0180	Custom data fusion logic	The data fusion engine allows the customization of the data fusion logic, for example to combine multiple data fusion techniques at the same time and for the same purpose, in order to provide a single output to the operator
FEAT_0181	Data fusion recommendations	The data fusion engine produces recommendations or guidelines for the operators as a result of the fusion process.
FEAT_0182	Geographic data import	Data coming from geographic information systems could be used either for supporting the data fusion engine or for user visualization support

4.2 CONTROL STATION - WEB CLIENT

The following table shows the list of features that shall be implemented in the Control Station - Web Client. Each feature is mapped to features to be implemented in the MC on which it relies.

Key	Summary	Monitoring Centre Features
FEAT_0050	Login	FEAT_0016, FEAT_0021
FEAT_0051	CRUD user	FEAT_0016
FEAT_0054	CRUD role	FEAT_0015
FEAT_0059	Show data collected by devices	FEAT_0153
FEAT_0060	Filter device data by criteria: date range, device type, device id, alarm level, substance, substance category, location, full text	FEAT_0044, FEAT_0045, FEAT_0046, FEAT_0047, FEAT_0062, FEAT_0133, FEAT_0134, FEAT_0135, FEAT_0168
FEAT_0063	Paginate device data	FEAT_0153
FEAT_0064	Sort device data by column	FEAT_0153
FEAT_0067	Show predefined charts for filtered data	FEAT_0153
FEAT_0072	Show a navigable tree structure: mission - devices - sensors - alarms for filtered data	FEAT_0146
FEAT_0078	Session management	FEAT_0016
FEAT_0083	Assign role to user	FEAT_0080
FEAT_0084	Assign privileges (pre-defined) to user	FEAT_0019, FEAT_0082

FEAT_0085	Assign privileges (pre-defined) to role	FEAT_0018, FEAT_0081
FEAT_0086	CRUD mission	FEAT_0025
FEAT_0087	Show mission details, including devices, sensors and collected data	FEAT_0146
FEAT_0091	Page navigation	FEAT_0020
FEAT_0136	Report configuration & production	FEAT_0128
FEAT_0137	Report templates visualization	FEAT_0106
FEAT_0138	System configuration parameters	FEAT_0013
FEAT_0139	Alarm notification email configuration	FEAT_0140
FEAT_0141	Mission configuration import	FEAT_0012, FEAT_0097
FEAT_0142	Issue configuration command	FEAT_0011
FEAT_0143	Mission device health check	FEAT_0125
FEAT_0144	Devices health check	FEAT_0126
FEAT_0148	Visualize indicators for filtered data	FEAT_0065
FEAT_0154	Load third party data file	FEAT_0153
FEAT_0159	CRUD real-time mission data	FEAT_0157
FEAT_0170	CRUD LEAs	FEAT_0169
FEAT_0190	Receive recommendations from the data fusion engine	FEAT_0181

4.3 CONTROL STATION - ANDROID CLIENT

The next table marks all features of the Control Station - Web Client that require to be ported to the Control Station - Android Client.

Key	Summary	Control Station - Android Client Features
FEAT_0073	Login	FEAT_0050
FEAT_0074	Show data collected by devices	FEAT_0059
FEAT_0075	Filter device data by criteria: date range, device type, device id, mission, alarm level, substance, location, full text	FEAT_0060
FEAT_0160	Paginate device data	FEAT_0063
FEAT_0161	Sort device data by column	FEAT_0064
FEAT_0077	Show a navigable tree structure: mission - devices - sensors - alarms for filtered data	FEAT_0072
FEAT_0162	Session management	FEAT_0078
FEAT_0076	Show mission details, including devices, sensors and collected data	FEAT_0087

FEAT_0164	Page navigation	FEAT_0091
FEAT_0093	Issue configuration command	FEAT_0011
FEAT_0094	Mission device health check	FEAT_0143
FEAT_0166	Operator devices health check	FEAT_0144
FEAT_0167	Visualize indicators for filtered data	FEAT_0148

In addition to the listed features, two additional capabilities should be implemented in the Control Station - Android Client:

Key	Summary	Monitoring Centre Features
FEAT_0079	Real-time data visualization	FEAT_0158
FEAT_0165	Issue configuration commands transparently to the user	FEAT_0142

5 HARDWARE REQUIREMENTS

The hardware to support the previously specified software requirements shall include network devices, servers, storage devices, personal computers and mobile devices. Furthermore, it shall support development and operations at the same time. In fact, according to the Description of Action of this project, during the two last year of the projects the data fusion engine will evolve and will be tuned by leveraging the outputs of the field tests. This means that, while the operations will be running and using the data fusion, also the development team will need to work on data fusion.

To support this runtime architecture, the following components are needed:

- Six rack server:
  - Four rack servers will be used for the operations and field tests, so to ensure:
    - availability;
    - performance;
    - scalability.
  - Two rack servers will be used for test and development. At least 2 servers are required to test the interaction between components that will be deployed on physically different servers in production.
- Two switches: one for runtime and one as a backup. The switch is a single point of failure and the second switch is required to minimize downtime in case of failure of the installed switch.
- One storage SAN: required to store collected data.
- Six smartphones: 4 for deployment and 2 for development and tests.
- Five laptops: 3 for deployment and 2 for development, tests and documentation

Such hardware devices allows to configure a test and development environment similar enough to the deployment environment used during the field tests, and having both environments running at the same time during the project.