ASSISTANCE

Adapted situation awareneSS tools and tallored training curricula for increaSing capabiliTie and enhANcing the proteCtion of first respondErs

European Commission

Project co-funded by the European Union within the Horizon 2020 Programme

assistance

Project Ref. N°	ASSISTANCE H2020 - 832576
Start Date / Duration	May 1, 2019 (36 months)
Dissemination Level[1]	PU (Public)
Author / Organisation	UPVLC

Deliverable D1.2

Data Management Plan

31/10/2019

[1] PU: Public; PP: Restricted to other programme participants (including the EC services); RE: Restricted to a group specified by the Consortium (including the EC services); CO: Confidential, only for members of the Consortium (including the EC services).

ASSISTANCE

Nowadays different first responder (FR) organizations cooperate together to face large and complex disasters that in some cases can be amplified due to new threats such as climate change in case of natural disasters (e.g. larger and more frequent floods and wild fires, etc) or the increase of radicalization in case of man-made disasters (e.g. arsonists that burn European forests, terrorist attacks coordinated across multiple European cities).

The impact of large disasters like these could have disastrous consequences for the European Member States and affect social well-being on a global level. Each type of FR organization (e.g. medical emergency services, fire and rescue services, law enforcement teams, civil protection professionals, etc.) that mitigate these kinds of events are exposed to unexpected dangers and new threats that can severely affect their personal safety.

ASSISTANCE proposes a holistic solution that will adapt a well-tested situation awareness (SA) application as the core of a wider SA platform. The new ASSISTANCE platform is capable of offering different configuration modes for providing the tailored information needed by each FR organization while they work together to mitigate the disaster (e.g. real time video and resources location for firefighters, evacuation route status for emergency health services and so on).

With this solution ASSISTANCE will enhance the SA of the responding organisations during their mitigation activities through the integration of new paradigms, tools and technologies (e.g. drones/robots equipped with a range of sensors, robust communications capabilities, etc.) with the main objective of increasing both their protection and their efficiency.

ASSISTANCE will also improve the skills and capabilities of the FRs through the establishment of a European advanced training network that will provide tailored training based on new learning approaches (e.g. virtual, mixed and/or augmented reality) adapted to each type of FR organizational need and the possibility of sharing virtual training environments, exchanging experiences and actuation procedures.

ASSISTANCE is funded by the Horizon 2020 Programme of the European Commission, in the topic of Critical Infrastructure Protection, grant agreement 832576.

Disclaimer

Executive Summary

This deliverable provides the ASSISTANCE Data Management Plan. It outlines how the research data collected or produced will be handled during and after the ASSISTANCE action, it describes which standards and methodology will be followed, and whether and how data will be shared.

This document will be updated over the course of the project whenever significant changes arise, such as new data or changes in the consortium policies or consortium composition.

List of Authors

Organisation	Authors
UPVLC	Federico Carvajal, Manuel Esteve, Israel Pérez, Débora Robles
E-LEX	Giovanni Maria Riccio
AVSRE	Jorge Martínez Rovira
SBFF	Mateusz Sosnowski

Change control datasheet

Version	Changes	Chapters	Pages	Date
0.1	First draft	All	16	25/09/19
0.2	Second Draft	All	21	04/10/19
Final	Final comments included	ALL	21	16/10/19

Content

List of Figures

No figures found.

List of Tables

Acronyms

ASSISTANCE	Adapted situation awareneSS tools and taIlored training curricula for increaSing capabiliTie and enhANcing the proteCtion of first respondErs
EC	European Commission
EU	European Union
CI	Critical Infrastructures
DMP	Data Management Plan
ICT	Information and Communication Technologies
WP	Work package
IPR	Intellectual and Property Rights

1. INTRODUCTION

1.1. ASSISTANCE Motivation

ASSISTANCE main objective is twofold, on the one hand the project will protect and help the different First Responders (FRs) organizations that work together during the mitigation of large disasters (Natural or Man-made) and on the other hand ASSISTANCE will improve the FRs capabilities and skills for facing these kinds of events.

Nowadays different FRs organizations cooperate together facing large and complex disasters, that in some cases can be amplified due to new threats such as, the climate change in case of natural disasters (e.g. big floods, large wild fires, etc) or the increase of radicalization in case of man-made disasters (e.g. pyromaniacs that burn European forest, big combined terrorist attacks in European cities).

The impact of these kinds of large disasters could have disastrous consequences for the European Member States' regions and social wellbeing in general. On the other hand, each type of FRs organizations (e.g. medical emergency services, firefighters' departments, law enforcement teams, civil protection professionals, etc.) that work mitigating these kinds of events are exposed to unexpected dangers or new threats that can severely affect their personal integrity.

Considering these facts, ASSISTANCE proposes a holistic solution that will adapt a well-tested SA application as a core of a wider SA platform, capable of offering different configuration modes for providing the tailored information outcome needed by each FR organization, while they work together mitigating the disaster (e.g. real time video and resources location for firefighters, evacuation routes status for emergency health services and so on).

With this solution ASSISTANCE will enhance the FRs SA during their mitigation activities through the integration of new paradigms, tools and technologies (e.g. drones/robots equipped with different sensors, robust communications capabilities, etc.) with the main objective of increasing both their protection and their efficiency.

On the other hand, ASSISTANCE also proposes to improve the FRs skills and capabilities through the establishment of a European advanced training network for FRs that will provide tailored training based on new learning approaches (e.g. virtual, mixed and/or augmented reality) adapted to each type of FRs organizations needs and the possibility of sharing virtual training environments, exchanging experiences and actuation procedures. ASSISTANCE has been financed by the Horizon 2020 initiative of the European Commission, in the topic SU-DRS02-2018, contract 832576.

1.2. Purpose of the Data Management Plan

The purpose of the Data Management Plan (DMP) is to provide an analysis of the main elements of the data management policy that will be used by the Consortium with regards to the project research data. The DMP covers the complete research data life cycle. However, since ASSISTANCE is not part of the Open Research Data Pilot (please refer to Article 29.3 of the Grant Agreement), no references to the management of the open access to research data are included in this document.

The DMP describes the types of documentation that will be generated or collected during the project, reflects the current state of the Consortium agreements on data management, and must be consistent with exploitation and IPR requirements.

In addition, The DMP identifies the requirements for accessing existing datasets that form the basis of the work of the project. Pertaining to the data that the project will produce, the DMP initially identifies the types of datasets that will be outcome of the project, namely: public deliverables, scientific publications, contributions to standards, software and applications. But these data may evolve during the project, e.g anonymized data traces from the transport and logistics use case.

This document is the first version of the DMP, delivered in Month 6 of the project. The DMP is not a fixed document and will be updated over the course of the project whenever significant changes arise, such as new data or changes in the consortium policies or consortium composition. The DMP will be updated before the periodic evaluation or assessment of the project as well as in time for the final review.

2. ASSISTANCE Datasets

A list of planned and expected datasets to be collected and produced during the ASSISTANCE project is presented below.

2.1. Data collected for analysis and evaluation

2.1.1. Personal Data

During the project duration, different information will be collected to:

- **Understand the FRs and their organisation.** Different FRs organizations will be interviewed by means of questionnaires and interviews, as part of the requirements collection phase of the project (T2.2). The objective of these questionnaires will be to better understand and assess the FRs end-user requirements and needs related to the scope of ASSISTANCE.
- **Develop Pilot Scenarios.** Different personal data (mainly images) will be collected and processed in order to successfully develop the pilot case studies.

Personal data will be requested for only for the development of the pilot case studies. The data that could be collected and processed are:

- Name and surname of the participants
- Organisation type
- Position in the organisation
- Images of the participants to the pilot scenarios

The consortium ensures that all the personal data will be processed after data subjects had provided their consent and that no sensitive information personal data (e.g. health, sexual, lifestyle, ethnicity, political opinion, religious, or philosophical conviction) will be collected nor processed.

The ASSISTANCE consortium has prepared an information sheet and an informed consent form for the collection of data during the pilot phase. The partner in charge of the pilot case study will be responsible for safeguarding the data collected.

More information about how data will be collected and processed has been included in the deliverables referred to the ethics requirements (D10.2).

2.1.2. Users Requirements Data

The users requirements data will be managed through Volere tool in order to ensure that only the partners working in the action have access to it. More information on the security of the Volere tool and project repository is included in section 2.7.2.

2.2. Datasets produced during the project

All the datasets used during the project (mainly generated in the project pilots) will be shared with the partners through the GIT repository or storing in secure databases prior authorisation of the disclosing partner.

2.3. Deliverables

Each deliverable has been classified following its dissemination level:

- **Classified, under level RESTREINT UE** (as per Commission Decision 2015/444/EC): if its unauthorised disclosure could be disadvantageous to the interests of the European Union or of one or more of the Member States.

  The deliverables classified as Restreint UE will require a special utilisation and treatment by project partners. On this ground, a Security Advisory Board was set during the first Project Steering meeting. One representative by organisation was designated and the police officer Raul Calderón, from MIR-PN, was appointed as Project Security Officer. He will be in charge of ensuring that all the security procedures are followed by all the project members in order to preserve the confidentiality of the information treated by the consortium during and after the project duration.

  The consortium will be in close contact with the National Security Authorities and will follow all the recommendations given by them in order to safeguard confidential information, specially the one considered in the Grant Agreement as Classified Information (restreint EU). All of this will be done under the coordination of the Project Security Officer.

  As part of the measures primarily focused on preserving the classified information, the following procedures have been set:

  - The partners concerned will maintain a record of the employees taking part in the project and will restrict the access to the classified information to them.
  - EU classification documentation will be marked as “restreint EU”
  - The partners will be trained on how to handle the EU classified information, how to use it, how to preserve its security and how to deal with any loss or unauthorised disclosure.

  These measures will be reminded in every Project Monitoring Committee.

  The Project Advisory Board members will not have access to any Classified Information (restreint EU).

- **Confidential, only for members of the consortium (including the Commission Services)**: The confidential deliverables will not be available on the website. In case of request from any external party, the Security Advisory Board may decide to disseminate the corresponding deliverables or specific parts of the deliverables to particular external parties.
  The Advisory Board members will only have access to the confidential documentation prior signature of a non-disclosure agreement.

- **Public:** The public project deliverables will be available for the public at the ASSISTANCE project website https://assistance-project.eu, in the Dissemination section. They will be uploaded to the website in pdf format after being approved by the consortium, the Security Advisory Board, and having been submitted to the European Commission.

The classification of the deliverables to be produced during the project are listed below.

Del. Nº	Deliverable name	WP Nº	Type[2]	Dissem Level[3]
D1.1	Project management handbook	WP1	R	PU
D1.2	Data Management Plan	WP1	R	PU
D1.3	Risk & Opportunities Register	WP1	R	PU
D1.4	First Annual Management Report	WP1	R	PU
D1.5	Second Annual Management Report	WP1	R	PU
D1.6	Final Management Report	WP1	R	PU
D2.1	Desk-Research Analysis and Identification of SA and Training Tools	WP2	R	PU
D2.2	User Requirements Specification	WP2	R	PU
D2.3	ASSISTANCE Reference Scenarios and Pilot Experiments specifications	WP2	R	CO
D2.4	ASSISTANCE System and Network Architecture Design	WP2	R	CO
D3.1	Sensor Abstraction Service Adapted Interfaces Definition	WP3	R	CO
D3.2	Sensor Abstraction Service Implementation	WP3	R	CO

[2] R: Document, report (excluding the periodic and final reports), DEM: Demonstrator, pilot, prototype, plan designs, DEC: Websites, patents filing, press & media actions, videos, etc., OTHER: Software, technical diagram, etc.

[3] PU: Public, fully open, e.g. web, CO: Confidential, restricted under conditions set out in Model Grant Agreement, CI: Classified, information as referred to in Commission Decision 2001/844/EC.

D3.3	Robust Mobile Communications	WP3	DEM	CO
D4.1	Adapted unmanned platforms	WP4	DEM	PU
D4.2	UAVs integrated into the system	WP4	OTHER	PU
D4.3	Robots integrated into the system	WP4	OTHER	PU
D4.4	Wearable Sensors integrated into the system	WP4	OTHER	CO
D4.5	Advanced UAVs capabilities	WP4	OTHER	CO
D4.6	Mission planner	WP4	OTHER	PU
D5.1	ASSISTANCE SA platform adaptation	WP5	R	PU
D5.2	ASSISTANCE SA advanced modules development	WP5	R	PU
D5.3	Robust Land Mobile Communications Infrastructure Development	WP5	DEM	PU
D5.4	Final SA Platform Integration	WP5	DEM	PU
D6.1	Training methodologies and evaluation criteria definition	WP6	R	PU
D6.2	Training curricula development and scheduling	WP6	R	PU
D6.3	Training scenarios and VR platforms setup	WP6	DEM	CO
D6.4	Training network establishment & pilots' evaluation	WP6	DEM	CO
D7.1	Validation Plan Report	WP7	R	PU
D7.2	Integrated System Test bed	WP7	R	CO
D7.3	First Pilot Summary Report and System Development	WP7	DEM	CO
D7.4	Second Pilot Summary Report and System Development	WP7	DEM	CO
D7.5	Third Pilot Summary Report and System Development	WP7	DEM	CO
D7.6	Evaluation Report	WP7	R	PU
D8.1	Report on the relevant legal EU framework and assessment of the ethical impact	WP8	R	PU
D8.2	Progress report on Gender Dimension Strategy	WP8	R	PU
D8.3	3 Progress report on Human Factor in ASSISTANCE impact assessment	WP8	R	PU
D8.4	Report on Gender Dimension Strategy GDS	WP8	R	PU
D8.5	Report on data protection, privacy & ethical impact	WP8	R	PU
D8.6	Best practices Handbook	WP8	R	PU
D8.7	Human Factor impact assessment	WP8	R	PU
D9.1	Project website	WP9	DEC	PU

D9.2	Updated Exploitation and Dissemination plan	WP9	R	PU
D9.3	Mid-term Dissemination Report	WP9	R	PU
D9.4	Research data management, Open Data and Open Access strategy	WP9	R	PU
D9.5	Final Dissemination Report	WP9	R	PU
D9.6	PCP and PPI preparation Plan for Commercialisation and Market Entry	WP9	R	PU

Table 1 Project deliverables classification according to their dissemination level

2.4. Scientific publications

The scientific publications, mainly scientific papers, created by the consortium members, will contain technical results from the ASSISTANCE project. These publications will be usually made available to a wide public audience. Restricted access to the publications will be accepted only in case of justified objections expressed by the consortium members or publishers of the scientific papers, or if there are some restriction issues regarding copyright from the Editorial Company.

The consortium is strongly motivated to provide technological and scientific results major importance and interest to the scientific and industry communities. Different international journals and conferences with significant impact and broad public awareness have been identified. Activities conducted and results obtained within ASSISTANCE will be disseminated primarily through presentations at relevant conferences, fairs and meetings during the duration of the project. All dissemination activities will be carefully monitored by the Security Advisory Board.

Details on the scientific publication process, target journals, conferences and other dissemination events will be included in D9.2.- Updated Exploitation and Dissemination Plan (delivered in month 12 to EC) and in the dissemination reports that will be produced in month 18th and 36th.

2.5. Contribution to standards

In order to achieve a maximal impact of the activities and results, ASSISTANCE will establish synergies not only with the FRs organizations, but also the project will provide targeted inputs to standards and policy development, e.g., in standardization for a, to enhance the exploitation potential of the proposed solution.

Task 9.3, led by RISE, will define, select and adopt appropriate standards to maximise the exploitation potential for the project and ensuring that the project provides interoperable solutions and interfaces across different User platforms. Close contact with standardisation bodies will be established in order to collaborate with a joint

standardisation initiative between and within the targeted standardisation and regulation bodies.

2.6. Other communication tools

Besides the aforementioned scientific publications, the project will generate further publications and other project outcomes such as:

- Promotion material (website, brochures, roll-ups, posters, etc.).
- Press releases and further project announcements.
- White papers created by the consortium on particular subjects.
- Any further publication generated by the project.

The dissemination materials will be handled and stored in the adequate repository according to their nature. Non-confidential publications will be uploaded to the project website. All partners will be demanded to disseminate them through their company websites and social media.

2.7. Security Data Management

2.7.1. Cybersecurity Data Management

Different sensors and tools used in cyber security gather information related to different security aspects. For instance, network intrusion detection systems are rule or signature based and detect a threat depending on the content, source IP, destination IP, protocol used, … Anomaly based detection systems will raise an alert depending on what is known as normal behavior. Host intrusion detection systems, are continuously checking systems logs for unwanted access or checksums for integrity, so on, information gathered can be the user logon in the system or network as the Active Directory login. The common parameters gathered and showed as relevant information when an alert is raised are listed below.

- Alert metadata: Timestamp, sensor name, location, correlation rule triggered...
- IP addresses and ports: Source and destination IPs addresses are meaningful for further analysis and prevention.
- Protocol and user agent: Usually network detection rules are defined for a specific protocol or user agent.
- Payloads: Network packets payloads that matched with the regarding rule are partially stored. The request operation is logged, headers, hostname, user-agent, connection status, …
- User login name: Host intrusion based systems audit systems authentication and therefor the login user name is stored if it’s relevant for an alert.
- Log entries: Related log entries that triggered a rule are stored and shown in the alert.

- Vulnerabilities: Audits assessment are scheduled, so on, vulnerabilities detected are stored.
- Service name: If services availability are monitored, service name and status is logged accordingly. This can be a proper service or CPU load, disk usage, …
- Hostname: Network activity can be surveyed to look for new hosts discovered.
- MAC address: As mentioned above, new hosts added are detected through MAC and IP inspection on a network.
- Message content: For third parties intelligence gathering sources, the content of a twitter message, author, and all public information related can be stored for further reputation or awareness analysis.
- Indicators of Compromise (IoC): Usually virus signatures, MD5 hashes, malware file, URLs, domain names are identified as indicators of compromise and stored to be identified by the related rules.

2.7.2. Self Hosted GIT Service (GOGS) security measures

GOGS security measures in document content services comprises a combination of authentication and authorization with additional security policies that can be implemented.

Authentication is internal and password-based in order to validate that a user is who or what claim to be. GOGS uses cryptographic password hashing to securely store passwords with MD4 (Message Digest 4) and SHA256 hash algorithms, this functionality can be enhanced with the use of Bcrypt (adaptative hash function).

Authorization is based on ACLs (Access Control List) of one or more ACE (Access Control Entities). An ACE associates a single authority to a single permission group and states whether the permission is to be allowed or denied. Each node in the repository has an ACL used to assign permissions to users and groups.

Furthermore, **additional security policies** are set in GOGS to mitigate security attacks such as Cross-Site Request Forgery (CSRF), Iframes and phishing attack mitigation, and security filters and clickjacking mitigation.

Communication to GOGS site is done through Transport Layer Security v1.2 which provides privacy and data integrity. The handshake to secure the connection is done through a RSA 2048 bits (SHA256 with RSA) signature algorithm sent back in a form of a digital certificate.

2.7.3. Data Center security measures

UPVLC is currently hosting GOGS server in the Distributed Real Time System Lab. This lab is provided with the listed security measures.

Physical Measures

- Access control: Access is granted and registered through personal security cards authentication.
- Racks secured: Servers are disposed in racks with physical key access.
- Temperature and humidity: These parameters are monitored and controlled.
- Climate controlled environment: Data center climate control is supervised in order to grant optimal server operability.
- Fire detection and extinction system: Fire detection sensors are deployed and in case of fire alarm, extinction system is suffocation based.

Logical Measures

- Access register: Access to servers are registered and logged.
- Unique actors: Each server operator has unique user assigned, so on operations and access can be monitored.
- Backups: Data is backed up in Madrid S2 Grupo data center as scheduled tasks for critical hosts and a physical copy is made and stored in another location.
- Software updates: Servers operating systems are continuously checked for software updates.
- Secured communication channel: Servers are remotely accessed with secure protocols and communications are encrypted.

3. IPR management

The ASSISTANCE consortium will adopt the applicable IPR directives and regulations for Horizon 2020 by applying the principle of equality of all the partners towards the foreground knowledge and in full compliance with the general European Commission policies regarding ownership, exploitation rights and confidentiality.

Rights and obligations of the partners concerning dissemination of results are included in the Consortium Agreement of the project.

4. Responsibilities

Each ASSISTANCE partner has to respect the policies set out in this Data Management Plan. Datasets have to be managed and stored appropriately and in line with applicable legislation. The Coordinator, together with the partner in charge of Task 9.2 (Dissemination and Communication of Project Results), have a particular responsibility to ensure that data shared through the ASSISTANCE website are easily available, but also that back-ups are performed and that proprietary data are secured. UPVLC, in charge of the hosting of GOGS repository, will be in charge of ensuring that the documentation uploaded to the repository is safeguard.

Validation and registration of datasets and metadata is the responsibility of the partner that generates the data in the WP. Metadata constitutes an underlying definition or description of the datasets, and facilitate finding and working with particular instances of data. Backing up data for sharing through open access repositories is the responsibility of the partner possessing the data. Quality control of these data is the responsibility of the relevant WP leader, supported by the Project Coordinator.

If datasets are updated, the partner that possesses the data has the responsibility to manage the different versions and to make sure that the latest version is available in the case of publically available data. All partners must consult the concerned partner(s) before publishing data in an open domain that can be associated to an exploitable result.

The Security Advisory Board will be in charge of approving the publication of any documentation or information considered as foreground of the project.