ISITEP
D6.2.1 - OPEN PUBLIC FUNCTIONAL SPECIFICATIONS

Document Manager:	George Mitsopoulos	NETFI	Editor

Programme:	Inter System Interoperability for Tetra-TetraPol Networks
Project Acronym:	ISITEP
Contract Number:	312484
Project Coordinator:	FINMECCANICA
SP Leader:	NETFI

Document ID N°:	ISITEP_D6.2.1_20160321_V3.0	**Version:**	V3.0
Deliverable:	D6.2.1	**Date:**	21/03/2016
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	George MITSOPOULOS (NETFI)
Approved by(WP Leader):	Dimitris ANDROUTSOPOULOS (NETFI)
Approved by(SP Leader):	Dimitris ANDROUTSOPOULOS (NETFI)
Approved by(Coordinator)	Paolo DI MICHELE (FNM)
Security Approval (Advisory Board Coordinator)	Etienne LEZAACK (BFP)

CONTRIBUTING PARTNERS

Name	Company/Organization	Role/Title
Marianne STORROSTEN	DNK	Contributor
Anita GALIN	MSB	Contributor
Federica BATTISTI	RM3	Contributor
Claudia OLIVIERI, Federico FROSALI	FNM	Contributor

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
All Company's Project Managers	All involved companies	Members of the Steering Committee
Elina MANOVA	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V1.8	21/05/15	All	All	First issue
V2.0	04/02/16	All	All	Updated according to the remarks of the Commission after the 2nd Annual Review
V3.0	21/03/16	All	All	Updated according to the remarks of the Commission after Review

Publishable extended abstract

The aim of this document is to provide the overview and the technical description for the development of the training tools which will support the operation of ISITEP. On one side, it is the development of a training tool aiming to assist end users on the operation and management of TETRA/TETRAPOL terminals, that are different (different manufacturer, model) from those used in their own organization. On the other side, it is the development of a tool that will collect and provide the necessary information related to the organizational and operational methods that different PPDR first responder agencies, from different European countries, employ.

Security Release Statement (by Etienne LEZAACK - Advisory Board Coordinator)

This document is classified as PUBLIC and there are no national security sensitive issues inside it.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The aim of WP 6.2 Training and Simulation is to determine the specifications and develop the necessary training tools that will support the operation of ISITEP[7][8].

On one side, there will be provided the technical description of the development of a training tool aiming to assist end users on the operation and management of TETRA/TETRAPOL terminals, that are different (different manufacturer, model) from those used in their own organization[5]. This will help the users participating in the operations to get familiar with the different type of TETRA/TETRAPOL terminals and their functionalities and provide a solid preparation for the demonstrations. In this case, it is anticipated that an application will be designed and implemented, that will visualize the functionalities of the user terminals employed within all different security forces participating in the demonstrations. Scope of this tool is to provide a user-friendly training platform to end users that visit a foreign European country and will potentially need to use an otherwise unknown to them TETRA/TETRAPOL terminal. The tool will also integrate all enhanced terminal capabilities developed within SP5 in order to facilitate their use by the corresponding end users.

On the other side, it is the technical description of the development of a tool that will collect and provide the necessary information related to the organizational and operational methods that different PPDR first responder agencies, from different European countries, employ. This will help the preparation of the different operations and contribute in the harmonization of actions of the different PPDR first responder agencies from different countries. In this case, the training tool that will be developed will aim to educate and train the end users on the organizational structure, methods and procedures that foreign PPDR forces employ in particular crisis situations. The tool will have the relevant information originating from all PPDR forces involved, stored in a database that through a user-friendly GUI will be easily accessed by Police, Fire brigade and other agency officers, to facilitate the more efficient cooperation with their foreign colleagues.

The aforementioned tools will support the interoperability of European PPDR forces, not only in the technical level but to operational and organizational level as well.

The present report is focused on defining all functional elements that will constitute the handheld terminal training tool and operations training tools. This will include :

- Specification of handheld terminal training tool aspects
- Specification of End-user Organizational and Operational training tool aspects
- Specification of Technical Requirements for both tools
- Specification of Graphical User Interface for both tools
- Definition of the Open Public Functional Specification for both tools

2. DOCUMENT SCOPE

In order to achieve theabovementioned goals, this document is organized to the following parts:

- **Section 4**: in this chapter, the system overview as well as its technical description of both tools is presented
- **Section 5:** The Specifications of Terminal Operation Aspects is presented.
- **Section 6**: The Specifications of End-user Organizational and Operational aspects is presented
- **Section 7:** The Specifications of technical requirements are described.
- **Section 8**: The Specification of Graphical User Interface
- **Section 9:** In this part reader can see the Open Public Functional Specification for both tools.
- **Section 10:** In this part the Organization and the Project Management of the software development is analysed.

3. DEFINITIONS AND ABBREVIATIONS

This section is intended to capture the definitions of some key terms used in the document for the purpose of increased consistency. Most of the definitions are obtained from official 3GPP and ETSI documents:

Access control: The prevention of unauthorized use of resources, including the use of a resource in an unauthorized manner.

Authentication: The act of positively verifying that the true identity of an entity (network, user) is the same as the claimed identity.

Confidentiality: The property that information may not be available or disclosed to unauthorized individuals, entities or processes.

Data integrity: The property that data has not been altered or destroyed in an unauthorized manner.

Encryption: The conversion of plaintext to cipher text.

Key: A sequence of symbols that controls the operations of encipherment and decipherment.

Key management: The generation, selection, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

Migration: Act of changing to a location area in another network (either with different Mobile Network Code and/or Mobile Country Code) where the user does not have subscription (e.g. ITSI in TETRA) for that network. In this document, migration is used as a synonym of roaming.

Profile: The capability of particular equipment. This is defined separately for individual subscriber terminals and individual infrastructures.

Provision: The act of supplying a given service (Note: A communication system may be capable of supporting a service. However, it may not supply the service to certain subscriber terminals for which the service is not subscribed.

The abbreviations of the current document are the following:

DBMS: database management system

PPDR: Public Protection and Disaster Relief

TETRA: Terrestrial Trunked Radio

SOP: Standard Operational Procedures

TSL: Transport Layer Security

SSL: Secure Sockets Layer

HTTPS: Hypertext Transfer Protocol Secure

4. THE SYSTEM OVERVIEW

4.1 The basic architecture

Two separated training tools will be developed, namely **train.TETRA**and **F.R.TETRA**(**First Response TETRA**). The first one, that will be called **train.TETRA**, will be developed for the purpose of the training tool aiming to assist end users on the operation and management of TETRA/TETRAPOL terminals, that are different (different manufacturer, model) from those used in their home organization. The second one, that will be called **F.R.TETRA** (**First Response TETRA**), will collect and provide the necessary information related to the organizational and operational methods that different PPDR first responder agencies, from different European countries, employ. This will help the preparation of the different operations to be performed during the demonstrations and contribute in the harmonization of actions of the different PPDR first responder agencies from different countries. These tools would be intergraded, from a technical point of view, as a **uni.TETRA** system**,** named by the words **united** and **TETRA.** Both tools would be accessed from an entrance web page. The basic architecture scheme is given to the following figure.

The approach of developing the system as a web-based application is preferred, instead of a desktop application. This approach is selected because of its advantages [8][4] in crucial aspects of the development, namely Scalability and Maintenance, Portability and Security. In particular:

- **Maintenance/Scalability** – A web-based application is to be installed only once and does not require installation at client-side, whereas desktop applications have to be installed separately on each end-user device. Therefore, the project is detached from installation-related issues, such as software and hardware incompatibilities and IT resources. Furthermore updating the application is cumbersome with desktop applications, as it needs to be done on every single machine, which is not the case with web applications where the most updated platform release is instantly available to the end-user.
- **Ease of use/ Portability** – It ensures that the system makes it convenient for the users to access the application from any location using the Internet.
- **Security** - A total control and special technologies is designed to be used, to protect it from various vulnerabilities in a better way than a standalone application that will download all sensitive data in a single point[11], [1].

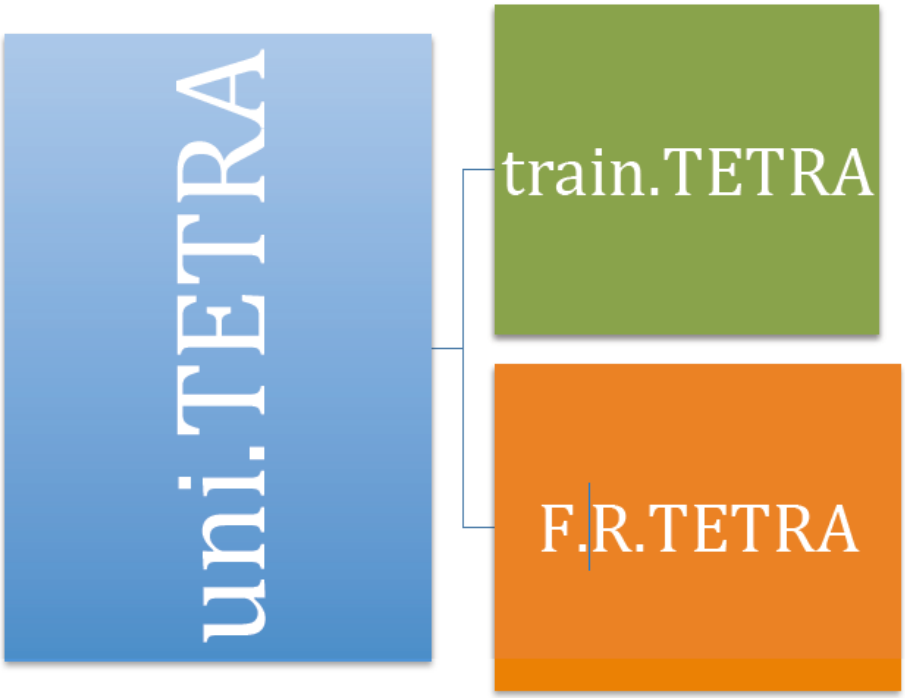

Figure 1.The uni.TETRAsystem's basic structure

The simplified description of each tool of the **uni.TETRA** is provided in the next paragraphs.

4.1.1 The basic architecture of the train.TETRA

The basic architecture of the **train.TETRA** tool is the following:

- **The storing Subsystem (Servers and Databases):** All the necessary information for the training will be stored into this system. The users must be considered as the clients of the server's application.
- **Front-end Subsystem:** This subsystem displays the training material. This subsystem interacts with the trainee users and users that will be the possible administrative authorities and maintenance services. Training references will be grouped into categories according to the origin of each trainee.
- **Back-end Subsystem:** This subsystem interacts with users that will be the possible administrative authorities and maintenance services.

The general scheme of the system is presented in the next figure.

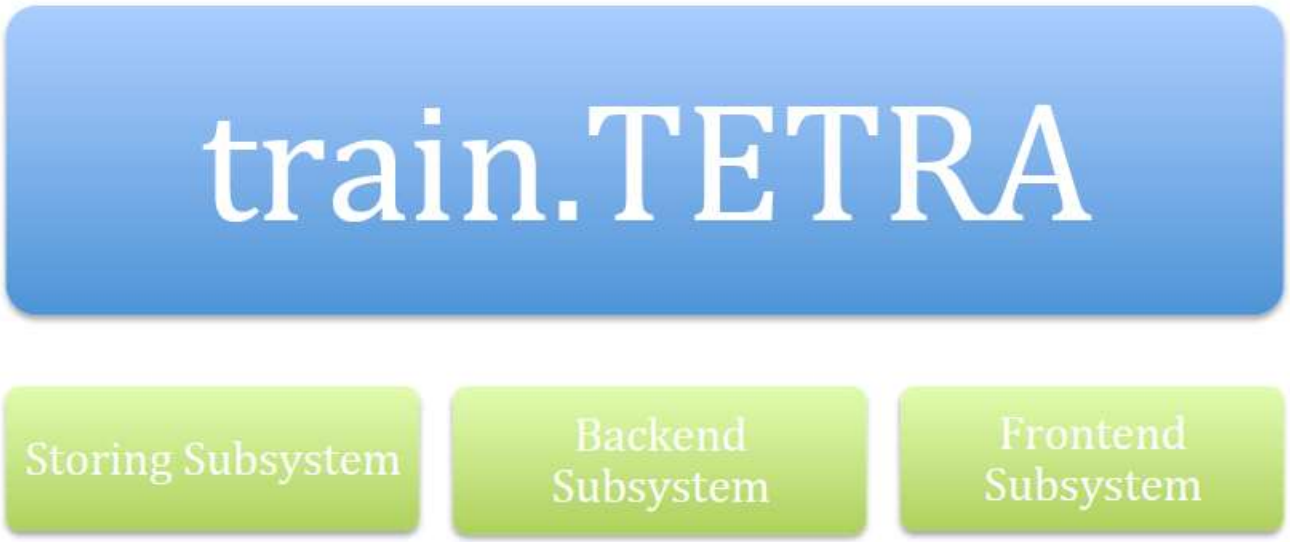

Figure 2. The train.TETRA tool's architecture

4.1.2 The basic architecture of the F.R.TETRA

The basic architecture of the **F.R.TETRA** tool is the following:

- **The uploading and reporting storing Subsystem (Servers and Databases):** All the necessary information related to the organizational and operational methods that different PPDR first responder agencies, from different European countries, will be stored into this system. The users must be considered as the clients of the server's application.
- **Front-end Subsystem:** This subsystem interacts with the users. Posts' references will be grouped into categories. It will provide the necessary information related to the organizational and operational methods that different PPDR first responder agencies, from different European countries, employ.
- **Back-end Subsystem:** This subsystem interacts with users that will be the possible administrative authorities and maintenance services. There are two distinct levels: the administrative and the user levels.

The general scheme of the system is presented to the next figure.

Figure 3.The F.R TETRA tool's architecture

4.2 Technical Characteristics

The general characteristics of each aforementioned subsystem are analyzed into the next paragraphs.

Important note: additional to the below given general characteristics, there are major interdependencies of the current WP 6.2 with the previously-deployed Work Packages **WP 2.1 Scenarios** and **WP 2.2.3 Requirements**, that may affect training content as well as development requirements and needs.

Servers and databases subsystem:

- This subsystem is a web server based on open source software (apache & tomcat) [2], and can be installed to whatever operating systems are selected. For the current prototype, a simplified Linux OS is used. The web server could be accessible via any on-line device, PC, notebook, smart phones, tablets etc.
- The web server supports secure HTTPs connection to all users.
- The web server has embedded the functions and tools needed to store, analyze, and display geographic information.
- Training data and other data is stored into a DBMS.
- The open source SQL database software will be used for developing the prototype application[9].

Front-end Subsystem:

- Using appropriate languages, like PHP[10], ASP [3], NET and JavaScript, will program the front end.
- It should have user-friendly, intuitive visual design.
- The user Interface accessible via any on-line device (PC, mobile, tablet), major Operating Systems and web browsers.
- Visuals, Look-and-feel, work-flows will be consistent to the standards used in TETRA /

TETRAPOL terminals.

- Will allow users to send feedback / comments to administrators
- Will allow users to access platform's support service, for inquiries regarding proper platform usage.
- Will support multi-lingual content and the tool UI will be in English.

Back-end Subsystem:

- The Back-end will be programmed by using appropriate languages, like PHP, ASP, .NET and Java-Script.
- This subsystem will enable administrators to manage the training material as also the other data /or information needed for the information related to the organizational and operational methods that different PPDR first responder agencies, by using an easy and flexible interface, adaptable to the device connected.
- Will collect and report feedback sent from front-end users – trainees.

4.3 The systems' users

The main categories of users are:

1. Visitors (non-authorized users, general public)
2. Authorized Users
    - Deployable PPDR Personnel
    - Organization/Agencies
    - Officer in Charge (OIC)
    - Non deployable PPDR Personnel
3. Administrators

5. THE SPECIFICATION OF HANDHELD TERMINAL TRAINING TOOL ASPECTS

5.1 Training Tool

The training tool, **train.TETRA**, will include the following parts:

- Content distribution subsystem, which will implement the necessary functions for the web availability of the system content to end users through appropriate graphical interfaces.
- Entities Management Subsystem, which will allow the management of the main entities of the platform i.e. the content, users and roles, work-flows and links between them.
- Handheld terminals visualisation training tool

The training application will include the following main features:

- Web based application for easy access from everywhere.
- Modular architecture in order to be able to host more devices in the future.
- Architecture that will allow simulating, theoretically, unlimited functions and unlimited devices.
- Hint/Help on every screen in order to guide and train users.
- Menu that will allow the user to jump to the functions that he/she wants to see/learn for a specific device.

Moreover, the application's main technical characteristics is the integration of the PHP programming language, the support of MySQL database for a lightweight CMS and JQuery mobile for the GUI. More specifically:

Server Requirements

Apache Web Server, PHP version 5.6+, MySQL Community Server vs 5.6+.

Minimum 2GB RAM, 4GB Free Disk Space

Client (user) Requirements

The system will be tested in various current browsers, like Google Chrome v47 and with Internet Explorer v11, but it should work on any device with a modern browser.

Set Up instructions

1. Create the database. Use a tool like phpMyAdmin[12]to run the setup.sql script located in your "SQL" folder.

2. Edit the "functions_settings.php" file located in the "html" folder with a text editor like notepad and set your database connection settings, server paths and contact form e-mails.

3. Upload the content of the "html" folder to the root of your web server.

4. Point your browser to the tool URL and login with e-mail admin@admin.com and password "admin". Use the "user management" tab to change admin e-mail and password.

Back up instructions

1. Export the database with a tool like phpMyAdmin[12].
2. Copy the contents of your root file folder.

Administration

From "admin" tab you can manually run the "cron_jobs.php" that performs the following actions

-Deletes temporary registrations

-Deletes temporary password change requests

-Deletes temporary email change requests

-Deletes old chat messages

-Add/edit content taxonomy terms.

-View platform details as number of users, content items, groups and training paths.

5.2 Handheld terminal visualisation training

This feature will visualise the functionalities of the user terminals employed within all different security forces participating in the operations. Scope of this tool is to provide a user-friendly training capability to end users that visit a foreign European country and will potentially need to use an otherwise unknown to them TETRA/TETRAPOL terminal. On top of this, the tool will also integrate all enhanced terminal capabilities developed within ISITEP in order to facilitate their use by the corresponding end users.

It will be based on a user-friendly interface. The entrance will be done by the main platform and will be granted to all because the tool will not contain any kind of classified information. However, each user must sign up during his first visit, so that an individual account is created.

After entering the tool, the user will be able to choose the type of hand held terminal that would like to be trained of using two different drop-down lists. The first list will contain TETRA manufactures like SELEX,Sepura, Airbus, Motorola etc. and the second list that will be active after the choice concerning the manufacturer, will contain the most common hand held terminals of the chosen manufacturer as also the new ISITEP terminal.

The choice of the handheld type will drive the user at a graphic interface of the terminal where the users would be able to access the most common modes of the device. At the same interface there will be a “how to” menu that would allow the user instead of losing time trying to find out a certain action, being able to use the menu list about the actions needed for solving its situation.

The training concept will be very simple from the trainee’s point of view as the tool will be designed for rapid deployed forces allowing them to familiarize with other than common to their knowledge, TETRA devices.

After the tool will be accessed by the portable or desktop device, user can use the two modes of operation that will be supported:

- Mode 1. In this mode the trainee can use the training tool just like a real radio or dispatcher. Because the network is hypothetically exists, there is no fear of the trainee causing trouble in the real network. To get to know the radio the trainee may consult the built-in manual for self-training.
- Mode 2.The trainee performs a predefined series of tasks. The tool monitors whether a certain exercise has been completed and if there were any problems. This mode is very efficient in teaching basic skills required in the handling of the real device or dispatcher. Basic operations such as how to use different call types, how to change group/folder, how to activate/deactivate group scanning and how to send/receive status will be taught effectively using individual exercises.

. The logical sequence for the training is given into the following figure.

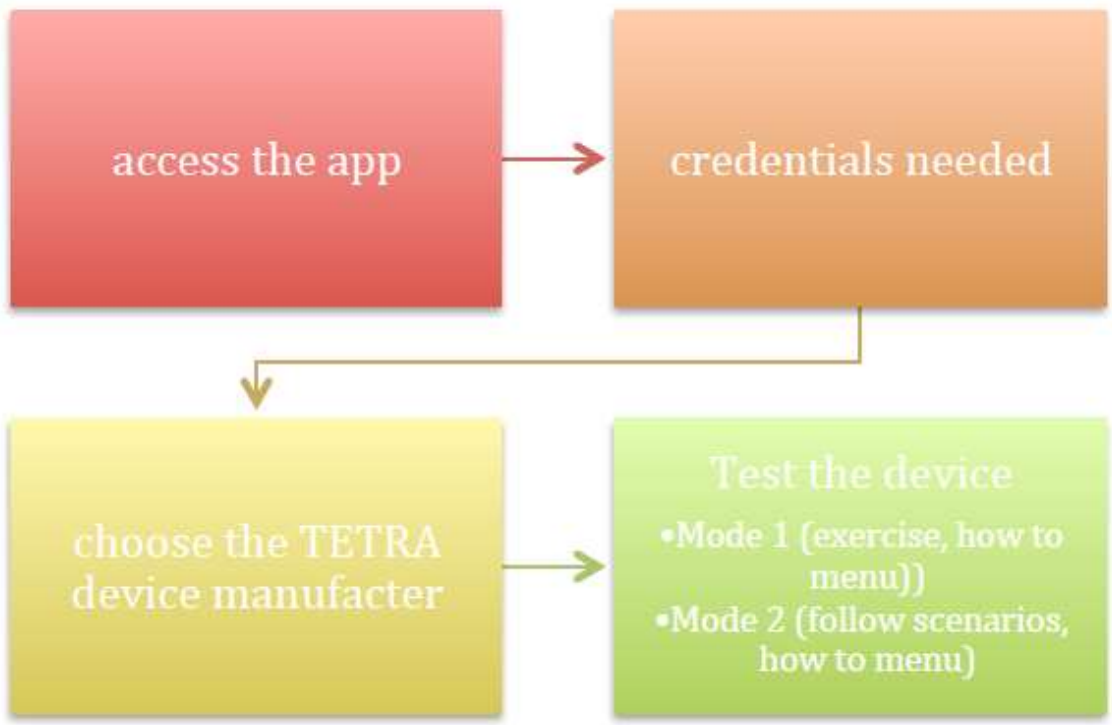

Figure 4.The train.TETRAtool logical navigation scheme

Individual User Accounts will be used for:

- Keeping updated user information, such as contact info, organization, country etc.
- Storing user preferences, such as preferred language
- Giving user the flexibility to continue training from different devices, like PC, laptop or mobile
- Provide administrative team with statics of usage per user / organization, reporting on progress of training programs etc.
- Platform's support service

Basic support should be provided to front-endusers, in terms of inquiries regarding the platform that occur while it's being used. Support requests can be submitted via a properly designed contact form, which will be accessible in the front-end. Support requests will be addressed by administrators, on given response times.

6. THE SPECIFICATION OF END-USER ORGANIZATIONAL AND OPERATIONALTRAINING TOOL ASPECTS

The **F.R.TETRA** tool will aim to educate and train the end users on the organizational structure, methods and procedures that foreign PPDR forces employ in particular crisis situations. The tool will have the relevant info originating from all PPDR forces involved, stored in a database that through a user friendly GUI will be easily accessed by Police, Fire brigade and other agencies officers, to facilitate the more efficient cooperation with their foreign colleagues.

The user's entrance to the **F.R.TETRA** tool will be controlled by a username and a password. The credentials will be based on the existence of the official agencies' e-mail that will be controlled. The user will be allowed to use the application by the administration team that will accept his access only after his registration is completed. If user has also an existing account in **train.TETRA**, same credentials will be utilized. In the **F.R.TETRA** application the user will use a friendly interface where he would be able to choose from a map the area where he is expected to deploy and the nation whose authority will be in charge of a current operation. A second screen will follow where the user will have the choice, in order to get familiar with the organization procedures of the nation in charge, to find:

- Standard operating procedures or Standard operating guidelines
- Phone call numbers.
- Organizational charts.
- Template reports.
- Hospitals, MEDEVAC procedures
- By-Laws and Constitutions
- Different agencies Mission Statement
- Strategic Plans
- Mutual Aid/Automatic Aid Agreements
- Regional Standard Operating Procedures/Protocols
- Laws, Regulations, and Standards
- Training Materials
- Special facilities/target hazards
- C4I details

The logical sequence for the **F.R.TETRA** is given into the following figure.

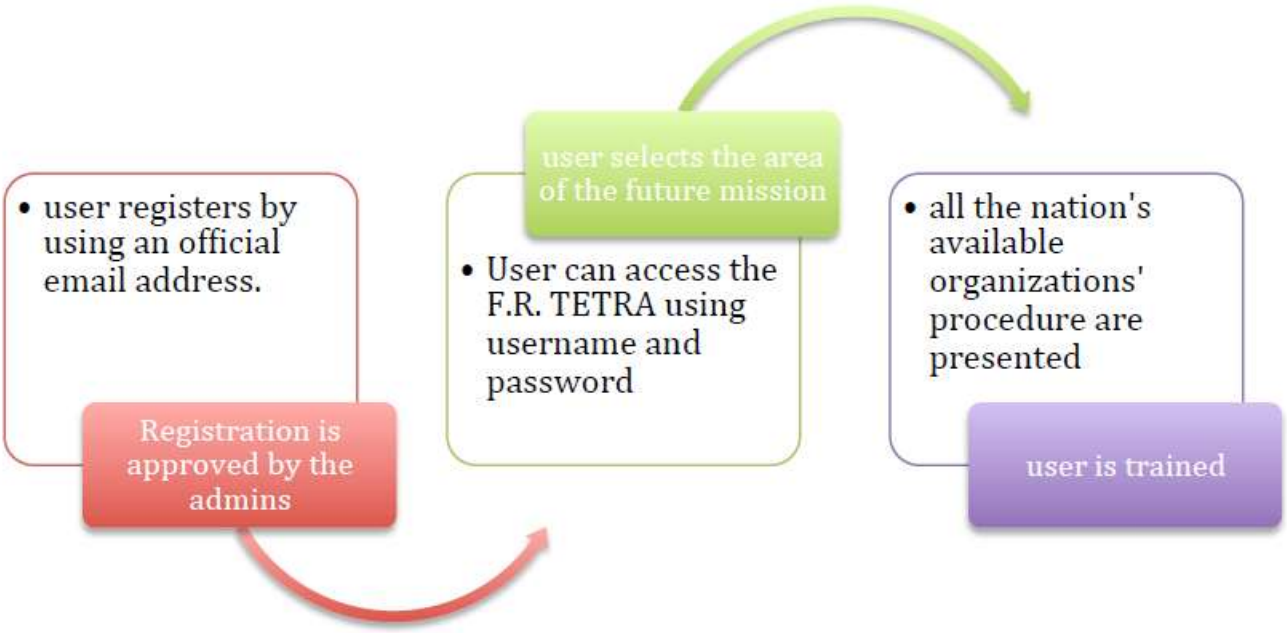

Figure 5. The F.R.TETRA logical operations

7. THE UNI.TETRASYSTEM'S TECHNICAL SPECIFICATIONS

7.1 General Idea

The tool will provide a single platform that allows rapid development of applications and subsystems with specific characteristics and requirements, enabling the interconnection and data exchange between subsystems and external systems in a common and consistent manner. The tool will be developed in programming environment using PHP and embedded .NET, .ASP and some JAVA.

The implementation environment will provide web services for different categories of users (Admin, Consultant, Deployed forces, Technicians, etc.) and services to the general public if required.

In terms of data management there will be a central point to record, manage and disseminate all the necessary information (data handheld specifications, Technical detail, Manuals, Organizational Charts, Procedures and SOPs etc.) required to avoid duplication and for the smooth operation of all structures. In any case, the information system will ensure the integrity and consistency of the data so the information for an entity will be kept at a single point in the system and will be updated only by the responsible structure and the corresponding subsystem.

7.2 System's technologies and principles

The designed system will cover at least the following technologies and implementation principles as shown in the table following.

Principle	Description
The system and all the subsystems will be fully interconnected	• It provides a modern design web-based environment for visitors and for authorized users • It uses a unified manner enforcement of policies (user roles, rights and authorizations, security, etc.) via Control and user access application • It provides a single implementation of the common data so that information for an entity to be kept at a single point in the whole system and created / updated only by the appropriate subsystem.
Open source software stack	The software platform as a whole and each of the subsystems will be able to work in open source software stack environment
Expandability, portability, flexibility	It will be based on a virtual simplified Linux machine.
Multilingual support	• The content will be multilingual. The user environment and the graphical interfaces will be available in English. • It support multilingualism at the data management level, ie the capacity to store values for each field of data entities in more than one language for all subsystems of the platform. • Integration in the graphic interfaces of on-line help at least in English language with the ability to further add extra languages

Table 1. System's principles and technologies

7.3 System's host minimum requirements

At a minimum system should be hosted on the following operating systems:

- Linux, CentOS, V6.2

- Windows Server, V 2008
- Microsoft Windows 7, Vista or XP

The hardware should meet the following requirements:

- Any normal server-station built after 2008 could run the Operation training tool(1 Ghz processor, 2048 MB RAM is required or minimum 2 Ghz processor, 4096 MB RAM are recommended)
- A least of 50 GB free hard disk space is needed.
- Monitor: A resolution of 1024x768 or more is required for local administrative purposes
- Network: a broadband connection is required in order the server be capable to perform all users' commands in time

Important note: additional to the below given general characteristics, there are major interdependencies of the current WP 6.2 with the previously-deployed Work Packages **WP 2.1 Scenarios** and **WP 2.2.3 Requirements**, that may affect workload and therefore system requirements.

7.4 System's end-users minimum requirements

The hardware is acquired by the end users and should meet the following requirements:

- Any normal PC built after 2005 could run the ISITEP training platform
  - 1 GHz processor, 512 MB RAM is required
  - 2 GHz processor, 1 GB RAM is recommended
- 100 MB free hard disk space is needed on each computer
- Monitor : A resolution of 1024x768 or more is required on each computer • A medium to large monitor is recommended for the trainer's computer
- Sound: A sound card and an optional headset, USB headsets are recommended because of an easier set-up and better compatibility
- Network: a common ADSL connection is required. No specific requirements

7.5 The technical and functional architecture

In general, the approach to be followed for the technical architecture of the **train.TETRA** and **F.R.TETRA** can be simulated by a model 3-tier model levels. The architecture includes

- A first layer, the data layer which gathers system data (eg databases, files, charts, etc.).
- A second level, the application layer, which provides the core of the system with respect to the functionality of it.
- A third level which allows the presentation and access to services to visitors, authorized PPDR personnel and administrators.

The functional architecture of the proposed system information consists of the applications:

- Data Management System: Direct access will have only the system administrator. Through suitably interface at least the following capabilities will be given to the admin:
  - Handheld terminal data management
  - SOPs, organizational charts, procedures data management

- Users data management

- Information System (Training Tools): In order the Information System to be completed, the data should be organized in a relational database (RDBMS). **Uni.TETRA** will be developed by a relational data model using relational SQL database.

- Security & Users Access that is analyzed in a next paragraph.

7.5.1 Security and users access applications

The criticality of the data integrity and the need for communication and information exchange with both between the subsystems and external systems requires the existence of a central Security and Access Control Subsystem. The use of the Information System subsystems will be determined depending on the role of each user (role-based access). User roles, their privileges and their data will be managed by a user management application. The application will set up user rights to data and apply its approval procedures and data management. The subsystem will manage secure access to authorized users in different types of information and functions of the system by authorizing and certifying users by checking the authenticity of the identity of the transacting parties (user authentication), in order then to allow the parties concerned to act on the authorizations they have.

To meet the functional needs of modern IT systems that leverage the technologies of the Internet, it is imperative to address a number of challenges relating to the security of the IT system, which is much more complex and difficult than the corresponding challenges faced by traditional client / server solutions.

System Security will be defined by this policy, which will be based on defined user roles and will be implemented through the safety and user access application. The requirements of security policy and related mechanisms have been defined through the following:

- The system security at applications level will be ensured through an authentication / authorization mechanism
- Access control operations, according to the user role. The definition of user rights will determine the actions a user can perform in relation to the data, functions and services supported by the system.
- Support of different user roles according to the indicative categories of users
- Roles and privileges are given and managed only by the system administrator and users are required to give 'username' and 'password' to access the system
- Support of the option that user has more than one role.
- Monitoring unauthorized access attempts and failed attempts per password or username.
- Block users after some consecutive failed attempts and inactive users after a preset period of inactivity
- Users never have direct access to the database. The application server through the relevant application has access to the RDBMS on behalf of the users.
- The system administrator may be able to monitor and record user activities in the system (monitor, control, notification, logging in).

Sensitive data managed by the system will be protected during their circulation in the network, but also during storage in databases, so as not to be readable and not being able not authorized users to alter or process them in an illegal manner. To ensure this the final app is using:

- Sophisticated encryption mechanisms based on powerful algorithms compliant with open standards. These mechanisms will allow both the encrypted transmission of communication

packet involving trafficked network data, and selectively encrypt certain sensitive data during storage.

- Furthermore, in the handling of data on the network, in the form of packet communication, a unique number (checksum) for each packet should be used for calculating the control algorithms and so that it is protected from unauthorized user wishing to interfere with the transmission, to alter and to retransmit.
- It is also necessary to ensure the end-to-end encryption within the multi-level (multi-tier) architecture of the Internet, regardless of the user's device, the type of network (wired, wireless etc.), communication protocols, the number of the involved application servers and database servers, the operating systems etc.
- Compliance with Protocol Transport Layer Security (TSL v1.1) or Secure Sockets Layer (SSL v3.0) and Hypertext Transfer Protocol Secure (HTTPS) when accessing the web servers.
- In order to ensure data availability, an information security mechanism will be implemented, at server level which includes at least an automatic backup of the parts of the platform (database, system files, etc) and system recovery mechanism to function after a disaster.
- Finally, the platform will have a level of achievement of the implementation mechanisms to shield from usual vulnerabilities in web applications usual categories attacks

7.6 Architecture

The three-tier architecture is selected for the system. This architecture attempts to overcome some of the limitations of the other schemes by separating the business application into three logical components: presentation, application logic, and data management. These logical components are “clean layered” in such a manner that each runs on a different machine or platform and communicates with the other components via the network[6].

In this client/server model, all the presentation logic resides on the client, all the application logic resides on multiple back-end application servers, and all the data management logic resides on multiple back-end database servers as shown in the next figures.

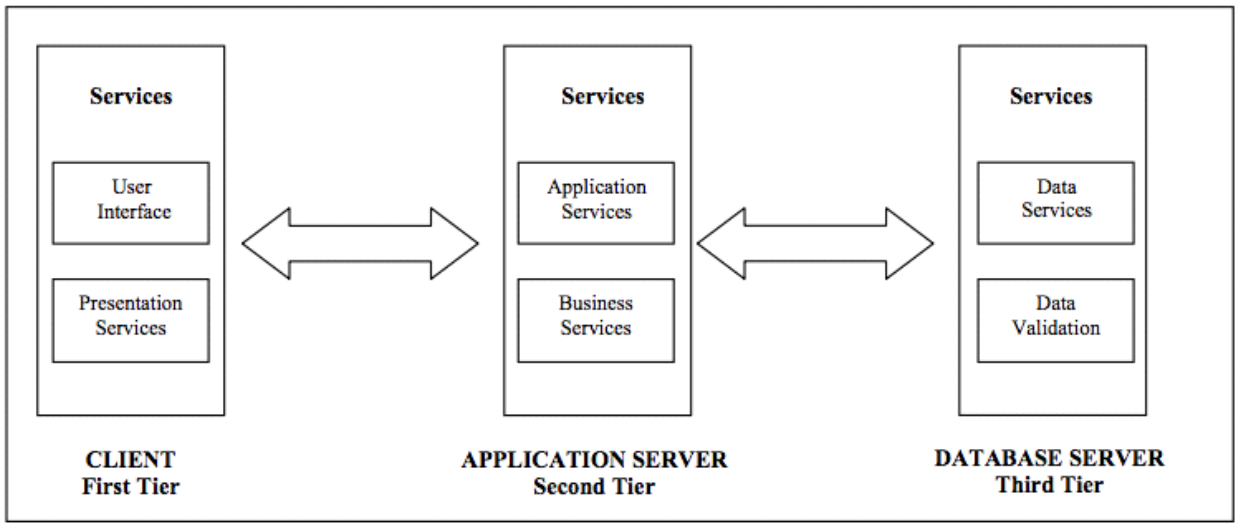

Figure 6. The 3-tier architecture scheme of the system

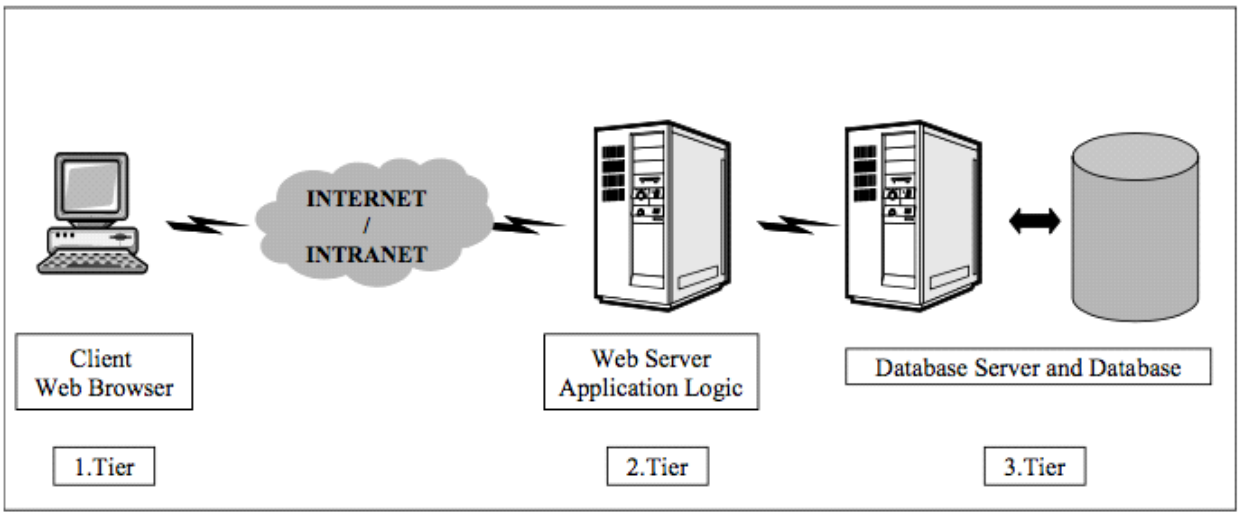

Figure 7. A more detailed 3-tier architecture scheme of the uni.TETRA system

7.7 Platform technical approach

7.7.1 Interoperability

Interoperability is defined as the ability of a system to work with other systems without requiring particular effort of the other part. In relation to interconnection, communication and interoperability with the external environment, the offered system will support open architectures and standards such as:

- Interoperability with third party systems through support protocols SOAP, WSDL and UUDI
- TCP / IP technology protocols support at both network and level application (IP v4, DNS, FTP, HTTP, SMTP / MIME, POP3, IMAP, LDAP v3)
- Content distribution via RSS

7.7.2 Multichannel approach

uni.TETRA will ensure multichannel approach of the Integrated System so as:

- The on-line use of platform and subsystems to be possible based on widespread web browsers (Internet Explorer, Mozilla, Chrome etc.) without restrictions on related software.
- The supported way of communication with the users will be the email, such as the user could be informed if required through automated message.
- The main way to access services is considered a web browser, as access terminals will be considered those that support the browser and it is a large range of devices (PC, laptop, tablet PC, smart phones, etc.).

7.8 Database Issues

As it has been already mentioned, the database will be implemented in MySQL. The final Database scheme will be decided according to the information delivered by the other interdependent WPs (**WP 2.1 Scenarios** and **WP 2.2.3 Requirements**). A generic database scheme is given for each subsystem in the next figures.

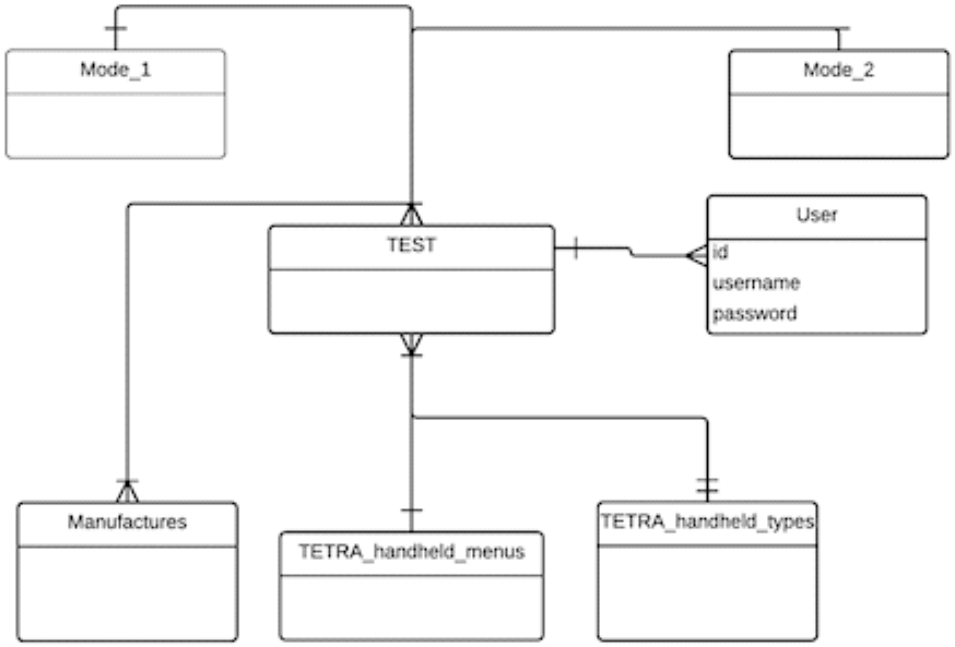

Figure 8. The database scheme of the train.TETRAtool

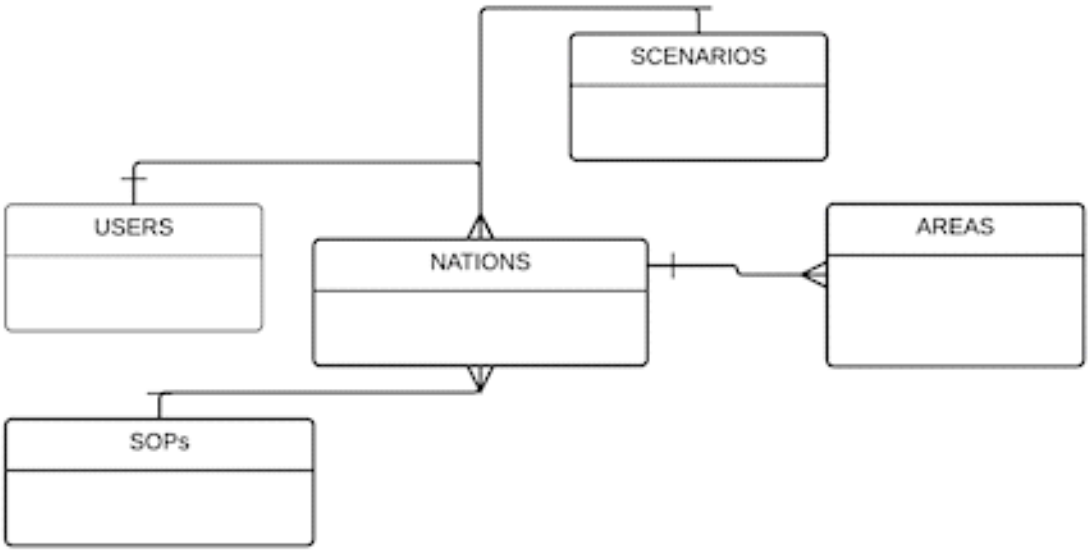

Figure 9. The database scheme of the F.R.TETRA tool

7.9 Final specifications frame

With regards to the requirements of the subsystems, the proposed architecture ensures at least the

followings:

- Development of subsystems using integrated definition process system.
- Development of subsystems using the Application Programming Interface for data manipulation
- Development of subsystems using the Remote Application Programming Interface for external development systems, which will benefit from the capabilities of the platform.
- Definition of an arbitrary number and data type, and the between them connections
- Definition of objects from combinations of basic types (eg String, Integer, Float, List), and other items that have been set
- Fully documented way to define and manage the types and data connections
- Control access to data through authorization system that takes into account the roles of the user, the subsystem and the types of data (authentication and authorization).
- Audit and logging mechanisms, which record the changes and users who perform them, in a manner that does not enable disclaimer (non-repudiation).
- Monitoring unauthorized access attempts and failed attempts per password
- Exclusion of users after some consecutive failed attempts and inactive users after a preset period of inactivity
- Use of Transport Layer Security (TSL v1.1) Protocol or Secure Sockets Layer (SSL v3.0) and Hypertext Transfer Protocol Secure (HTTPS) when accessing the web servers
- Automatic creation of the necessary storage structures after completing the definition of data fields and relationships between objects
- Access to the actions on behalf of the subsystems via fully documented API
- Delete: Under unique id
- Partial recovery: Under unique id. Recovered only the object and fields, without lists and sets of different objects with which it is associated
- Full recovery: Under unique id. Loads all objects that are connected to the object
- Search by queries understandable to the storage system
- Full description of the method for matching objects of the platform with the structures of the storage system, e.g. OR mapping, object serialization, etc.
- Creation in the definition processes and work-flows on the types of data set
- Graphical User Interface (GUI)
- Automatic generation of graphical user interface
- Data security Mechanism, which includes at least an automatic backup of the parts of the platform (database, system files, etc.) model and system recovery mechanism to function after a disaster.

7.10 Reporting export requirements

This subsystem will implement data export and reports which can be defined. This is a fully customizable report and statistics export system, which will ensure at least:

- Provide fully documented way of describing the data to be recovered as well as additional statistics calculated from these.
- To support a fully documented standard system (template) for determining the final version of the report.
- To offer the possibility of exporting reports in various formats and open standards HTML, XML, ODF, PDF
- To offer various options of delivering the reports (i.e. direct download, send as attachment in email recipients, schedule and auto send)
- Supported access control to the reports and the possibility for public reports, i.e. reports which could be assigned to trainees, organizations or the general public through the content distribution subsystem

8. THE SPECIFICATION OF GRAPHICAL USER INTERFACE

8.1 GUI security

All system users will enter the system with the identification process to verify their identity (authentication) and cannot access the data without authorization (authorization). It will support different user roles, determine access rights to data and functions in the system (accountability). The system will provide mechanisms for recording changes made, that will record the changes and admin who perform, in a manner that does not enable disclaimer (no repudiation). Additionally, the system will have data available (availability) to authorized users at the right time and in the appropriate format.

8.2 GUI accessibility

In the design of graphical user interfaces of the platform will take account of the specific needs and requirements of people with disabilities (PWD) guaranteeing their access through on-line services and content. Specifically, we will ensure full compliance and documentation that the accessibility guidelines Web Content Accessibility Guidelines at level AA (WCAG 2.0 level AA).

8.3 GUI ease of use

During system design we guarantee that we will follow the usability principles to ensure that the whole system is easy to use, with friendly interface, without requiring specific knowledge by users. Particular emphasis will be given to the end-user interface.

One of the most important parts of an information system is the user interface. The user interface is well designed to allow users to use the functions of the system; otherwise the system might not be functional.

The user interface is fully graphical (GUI) using all the known characteristics (mouse, windows, function menu, function buttons, selection lists, etc.).

The user interface will have a single design concept so do not confuse the user. This concerns the use of a common colour palette and the use of common notations for similar functions.

To that purpose, the various operations will have a logical sequence of steps to minimize the steps required to complete an operation, there will exist a clear indication the step that the user stands and how to proceed in next or previous step, there will be a clear indication of what page the user is located in, what was the path followed to reach and to what upper or lower level pages can be moved.

8.4 Platform operational approach

The platform will provide the environment for staff training in handheld terminals and operational procedures. The services will be provided through Web interface to all users involved in the operations as personalized on-line services, and the general public as general information services. The main users of the overall information system will be the staff of PPDR services.

9. DEFINITION OF THE OPEN PUBLIC FUNCTIONAL SPECIFICATION.

The system will be based on Open architecture, ensuring the following features:

- Use of open protocols for communication between levels (tiers) of the platform.
- Use of published programming interfaces for communication between different modules (modules) of the platform. Publication means the public access to the documentation of the interfaces and the corresponding specification files interfaces, for example in WDSL files for web services based on SOAP**.**
- Use of published programming interfaces for communication between the platform and the individual subsystems with third party systems as well as new elements that expand its functionality.
- Using open standards for the representation of the data exchanged via programming interfaces, between the subsystems of the platform and between the platform and the third external systems
- Independence from specific vendor's hardware, operating system and software.

10. ORGANIZATION AND PROJECT MANAGEMENT

10.1 Methods and Technical implementation and support

We will use modern methods referring to project implementation and technical support for:

- Management methodology and project monitoring
- Project Implementation Methodology to analyse all individual techniques will be used
- Quality Assurance Methodology

10.2 Project management & quality assurance

The implementation of the Quality Assurance System for the project will be achieved through a number of complementary measures, which in many cases coincide. These actions will be carried out by NETFI and will include as minimum:

- The design and implementation of quality assurance procedures for the precise definition of what is needed, by whom and standards by which the work is carried out for the project.
- Develop a team approach to review and improve the project implementation work.
- Quality control journal for measuring the effectiveness of internal processes in the achievement of performance targets.
- Periodic inspection of processes and deliverables for their agreement with the project Quality Plan that has been drawn up.
- Update of the project's organizational structure stakeholders on the results of quality control and corrective actions needed to be taken in the event of deviations from the original specifications.

These actions will be implemented during the project implementation:

- At the end of each phase of the project, during the inspection and evaluation of the phase deliverables.
- During the testing process, parts or the entire project, under the control of the test results and the recommendation to conduct new tests, where the need for corrective measures created.
- In the process of the final assessment of the project in the configuration recommendation for acceptance tests.
- During project implementation in the context of ensuring the implementation of quality assurance procedures of the parties involved.
- Within the organization and monitoring meetings with system users to ensure their satisfaction with the quality of work performed completeness, functionality and immediacy of operation.
- During the pilot operation of the system in the control and monitoring procedures to be applied.

10.3 Quality Control

Quality control criteria procedures that will be used:

- The smooth and on timely manner, flow of appropriate information to the appropriate people.
- The effectiveness of meetings and appointments (well-prepared, short duration, catalytic

coordination speeches and collected the necessary data to formulate practical decisions and avoid references to new meetings due to lack or negligence)

- Periodic approval of interim Deliverables.
- The efficiency of the working groups, which will begin on the timely completion and quality of deliverables, and the cooperation index of people who make up the.
- The timely completion of the work (on schedule)
- Defined Rules of approval of the deliverables

10.4 Indicative deliverables

Indicative Deliverables control criteria are:

- Meeting the requirements described,
- Functionality, usability, scalability, and reliability of the software tool that will be developed,
- Clarity, content and completeness of the documentation to be produced (issues Functional Specifications, User's Guide, etc.) and their compliance with predetermined document formats

10.5 The management of change and development within the project

This technique is used to form a coherent framework for the early detection and rational treatment of changes in a project, which may arise as a result of:

- Change on the specification of products / services of sub-projects
- A proposal for improvement of one or more tool (outcomes) of working packages,
- A proposal to amend the timetable for implementation,
- Failure of a product to comply with the quality criteria set, etc..

This technique provides for evaluation of the change request on the priority / urgency of implementing and assessing the benefits of its implementation and their effects in terms of cost, time and new risks for the project.

10.6 Risk Management System

The objective of Risk Management in the context of total quality approach is to anticipate and plan how to overcome and reduce the likelihood or risk mitigation techniques, which will have influence on the project.

Risk management as an idea must face and condemn the daily work of each member of the team. We use a systematic central planning at the outset of the project, continuous inspections and adjustments throughout the project duration[11].

The RMP is used by:

- Leader of Work Package
- Responsible personnel for subtasks
- Management team of the Project

Risk management is an integral component of Management and Project Planning. The Risk Response Plan is prepared at the early stages of the project to demonstrate and ensure that:

- The requirements and constraints of the contract have been reviewed.

- An effective Risk Management mechanism has developed.

The Risk Management Plan is initially included in the Project Implementation Plan, and systematically on Monthly Project Progress Reports and the internal project documentation.

Three main categories of risk can be determined for the project:

- Technology Concepts (software& hardware)
- Humanware
- Businessware.

The proposed Risk Management Methodology consists of a set of consecutive actions to be undertaken to identify, communicate and solve the risks of large IT projects. The model used to represent the commonly used methodology is a circular set of actions emphasizing that risk management is an ongoing process.

Our methodology includes the following steps:

- For each type (category) of risk potential risks identified.
- For each identified risk the following parameters are defined: severity, chance (probability), traceability (delectability) and ease of recovery (recoverability). Then calculate the total level of risk using the following equation:

Risk = Severity x Probability x [(Delectability + Recoverability) / 2]

- All parameters are graded on a scale from 1 to 10, where 10 is the worst rating (i.e. 10 means a high degree of probability of occurrence risk or very difficult recovery).
- Rating can also be done not only by defined risk, but also by risk category and overall.
- Risk assessment. The risk assessment results in the issuance of risk priorities, achieved through a comparison scale, probabilities (high, moderate, low) and their effects (impact)
- Addressing risks.

For a high risk for the project as staff turnover, for example, we recommend the following steps:

- Meeting with the existing staff to determine personnel change reasons.
- Action to eliminate these reasons, under direct control before starting the project.
- When project starts, assume that the staff changes will actually happen and made sure that there are standardized development procedures to ensure the continuation of the project.
- Organize working groups so that information for any development activity to be widely disseminated within the project as required.
- Determine documentation standards and establishing mechanisms to ensure that the documents will be delivered within deadlines and drawn uniformly.
- Run peer inspections (peer reviews) all the work so that the required members to be aware of the situation.
- Identify an alternate person for each critical position

11. REFERENCES

[1] Albakri, S., Shanmgam, B., Samy, G., Idris, N., & Ahmed, A. (2014). A case study for the cloud computing security threats in a governmental organization. IEEE.

[2] Apache Tomcat. (n.d.). Retrieved from Apache Tomcat: http://tomcat.apache.org/

[3] ASP.NET. (n.d.). Retrieved from ASP.NET: http://www.asp.net/

[4] Christian Baun, M. K. (2011). Cloud Computing: Web-Based Dynamic IT Services. Springer.

[5] ETSI EN 300 392-3-1 V1.3.1 (2010-08), “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 1: General design”. (n.d.).

[6] Goodyear. (2000). Enterprise System Architecture. CRC Press.

[7] ISITEP D24.1 v1.0, “System subsystem design description (SSDD) candidate Release”. (2014, September).

[8] Miller, M. (2009). Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate On-line. QUE.

[9] MySQL. (n.d.). Retrieved from MySQL: http://www.mysql.com/

[10] PHP: Hypertext Preprocessor. (n.d.). Retrieved from PHP: Hypertext Preprocessor: http://php.net/

[11] Shaikh, F. (2011). Security threats in cloud computing. IEEE.

[12] https://www.phpmyadmin.net/