This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 832981

Deliverable D4.2

Developed Web Collaborative Platform

Due date of deliverable: 31/08/2023

Actual submission date: 31/08/2023

George Kolev[1], Garik Markarian[1], Nataly Polushkina[1]

Laura Petersen[2], Grigore Havârneanu[2]

1: RINISOFT 2: UIC

The document reflects only the author’s views and the Commission will not be liable of any use that may be made of the information contained therein. The use of the content provided is at the sole risk of the user.

Project details

Project acronym	PROACTIVE
Project full title	**PR**eparedness against CBRNE threats through c**O**mmon **A**pproaches between security pra**CTI**tioners and the **V**uleranbl**E** civil society
Grant Agreement no.	832981
Call ID and Topic	H2020-SU-SEC-2018, Topic SU-FCT01-2018
Project Timeframe	01/05/2019 – 31/08/2023
Duration	52 Months
Coordinator	UIC – Grigore Havarneanu (havarneanu@uic.org)

Document details

Title	Developed Web Collaborative Platform
Work Package	WP4
Date of the document	31/08/2023
Version of the document	07
Responsible Partner	RINISOFT
Reviewing Partner	ETICAS, CBRNE, UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	01/07/2023	First Draft
02	15/07/2023	Second Draft
03	24/072023	Third Draft
04	01/08/2023	Fourth Draft released for Consortium comments and contributions
05	14/08/2023	Fifth Draft
06	21/08/2023	Final Draft
07	31/08/2023	Final Version

Consortium – List of partners

Partner no.	Short name	Name	Country
1	UIC	UNION INTERNATIONALE DES CHEMINS DE FER (COORDINATOR)	France
2	CBRNE	CBRNE LTD	UK
3	PPI	POPULATION PROTECTION INSTITUTE (MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC)	Czech Republic
4	DB	DEUTSCHE BAHN AG	Germany
6	UMU	UMEA UNIVERSITET	Sweden
7	DHPOL	DEUTSCHE HOCHSCHULE DER POLIZEI	Germany
8	RINISOFT	RINISOFT LTD	Bulgaria
9	WMP	WEST MIDLANDS POLICE AND CRIME COMMISSIONER	UK
10	ETICAS	ETICAS RESEARCH AND CONSULTING SL	Spain
11	SESU	STATE EMERGENCY SERVICE OF UKRAINE	Ukraine
12	UKHSA	UK HEALTH SECURITY AGENCY (DEPARTMENT OF HEALTH – PUBLIC HEALTH ENGLAND)	UK
13	SPL	STATE POLICE OF LATVIA	Latvia
14	AGS	AN GARDA SÍOCHÁNA – NATIONAL POLICE FORCE IRELAND	Ireland
15	FFI	FORSVARETS FORSKNINGSINSTITUTT	Norway
16	NPH	KOMENDA GŁÓWNA POLICJI	Poland

Executive summary

The purpose of this deliverable (D4.2) is to provide detailed description of the co-creation, testing and verification process used throughout the project to develop the PROACTIVE web collaborative platform. The PROACTIVE web collaborative platform is one of the three components of the PROACTIVE Crisis communication system that aims to facilitate communication between practitioners and citizens both before and during a CBRNe incident. The other two components of the system are the modular App for practitioners (D4.3) and the mobile App for vulnerable citizens (D5.4).

The development focused on ensuring that all the requirements, as defined in PROACTIVE policymaking toolkits, were met. This involved facilitating Law Enforcement Agencies (LEAs) and Security Policy Makers ability to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The developed platform helps to improve the efficiency of the communication between LEAs, Policy Makers and Citizens, with a particular focus on information sharing and usability by vulnerable groups (T5.4). The technology, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by mobile technologies, as well as modern data analytics capabilities to support users in overall decision-making processes. The provision of 'other applications' (such as Twitter, Facebook) has also been implemented, covering potentially any application outside of the PROACTIVE system, which may interact by pushing/pulling information to or from the PROACTIVE system.

Input from WP1, WP2, WP3, WP5 and WP8 has been reviewed to determine the needs and gaps of the users in terms of current public perceptions relating to Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) incidents. The research completed in WP1 will feed into the key engagement tasks in WP2 and WP3, and by default will provide key feedback for the Toolkits in WP4 and WP5. The work and deliverables completed in WP4 were utilised during the exercises in WP6. Feedbacks received from 3 PROACTIVE exercises helped to improve the developed platform, while inputs from WP8 and WP10 were utilised for evaluation of ethical and legal compliances. In addition, even though this was beyond the original scope of the PROACTIVE project, special emphases were made to ensure compliance with "Secure by Design" requirements.

The developed platform will remain active and usable for forceable future after the completion of the project. RINISOFT will continue maintenance of the developed software, ensuring that the whole PROACTIVE Crisis Communication System (both the web platform and apps) are still available on relevant third party servers and can support communication between practitioners and citizens beyond the life of the project.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Server
CBRNe	Chemical Biological, Radiological, Nuclear, explosive
CSAB	Civil Society Advisory Board
D	Deliverable
DPO	Data Protection Officer
DSDM	Dynamic Systems Development Method
FR	First Responders
GDPR	General Data Protection Regulation
GIS	Geographic Information System mapping
GUI	Graphic User Interface
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol Address
IPR	Intellectual Property Rights
LEAs	Law Enforcement Agencies
MoSCoW	Must have, Should have, Could have, and Won't have
PSAB	Practitioner Stakeholder Advisory Board
QA	Quality Assurance
REST	Representational State Transfer
SOP	Standard Operating Procedure
SQL	Structure Query Language
TLS	Transport Layer Security
UAT	User Acceptance Testing
WP	Work Package

1. INTRODUCTION

1.1. Project Summary

In line with the EU Action Plan to enhance preparedness against Chemical, Biological, Radiological Nuclear and explosive (CBRNe) security risks and the overall Security Union approach to fight crime and terrorism, PROACTIVE aimed to enhance societal CBRNe preparedness by increasing Practitioner effectiveness in communicating and managing large, diverse groups of people in a CBRNe environment.

This was achieved by delivering new PROACTIVE tools and providing innovative recommendations for Policy Makers and Safety and Security Practitioners. Liaising with the eNOTICE H2020 project, three joint exercises were conducted with special emphases on roles play by volunteers recruited by PROACTIVE and evaluation of the developed tools. These exercises helped to evaluate the acceptability and usability of existing procedures and test new tools developed within PROACTIVE,

One of the tools resulted from the PROACTIVE project is a CBRNe Crisis Communications System, which includes three core components:

- a Web Collaborative platform with database scenarios for LEAs and Security Policy makers
- an innovative response tool in the form of a Mobile Application for Practitioners
- a Mobile App for Vulnerable Citizens.

This PROACTIVE CBRNe Crisis Communications System was developed within WP4 of the project.

1.2. Objectives of WP4

The main objectives of WP4 were defined in the original project proposal and can be summarised as follows:

- Develop the comprehensive technological components supporting the Toolkit;
- Design the complete PROACTIVE CBRNe communications toolkit (set of tools and supporting technologies), ensuring modularity, flexibility adaptability, scalability, usability and robustness,
- Build technological tools facilitating communication and cooperation between LEAs and security-based policy makers in an efficient and effective way, exploiting the use of mobile technologies and bi-directional communication;
- Develop restricted access rich visualisation and reporting tools for LEAs and coordinating entities assisting security monitoring of communities; assessing risks, threats, vulnerabilities and incidents; allocation of resources and decision-making;
- Integrate, test and validate the Toolkit.

1.3. Objectives of D4.2

The key objective of D4.2 is to report on the design, development, implementation, testing and validation of the PROACTIVE CBRNe web collaborative platform for LEAs and Security Policy makers. The deliverable outlines the key results obtained throughout the project and documents these results for future use after the project completion.

2. PURPOSE OF THE DELIVERABLE

The PROACTIVE CBRNe web collaborative platform for LEAs and Security Policy makers is the main output of D4.2.

While this deliverable focuses specifically on the development of the web collaborative platform, it is important to note that the web platform is one component of the overall PROACTIVE Crisis Communication System. The PROACTIVE Crisis Communication System is made up of a:

- Web collaborative platform, with an intend end-users of LEAs and Security Policy Makers (this deliverable),
- Mobile App for Practitioners (D4.3) and
- Mobile App for vulnerable citizens (D5.4).

Hence, since the start, all three components have been developed in a harmonised way and all tools share common denominators as expressed in the initial architectural design documents. As shown in D4.1 & D5.3, the core structure of the system is the same across all three so as to enable consistency and bi-directional communication, while allowing customisations for specific groups of users (e.g., LEAs, Policy Makers, Citizens). They all aimed to ensure a modular, flexible, extensible, scalable, robust and secure system. The PROACTIVE Crisis Communication System, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by digital technologies, as well as modern data analytics capabilities to support the users in overall decision-making processes. Accessibility, in particular, is a key focus across the system as a whole. This is principally important for vulnerable communities or communities that are more difficult to reach; deaf, visually impaired, religious, children, elderly, etc. It is also important to ensure that the tools are accessible for all CBRNe practitioners. The provision of ‘other applications’ (for example Twitter, Facebook) has also been addressed and allows integration with third party applications, this covers any application outside of the PROACTIVE system, which may interact by pushing/pulling information to or from the PROACTIVE system.

The PROACTIVE CBRNe Crisis Communication System was developed based on the bellow requirements defined by the PROACTIVE project in consultation with all potential stakeholders:

- **User Experience**: The Platform should be designed with the user in mind, with an intuitive and user-friendly interface. The user should be able to easily navigate the Platform, access information, and complete tasks.

- **Functionality**: The Platform should have all the necessary features and functionalities, such as account management, and access to content and services.

- **Security**: The Platform should be designed with security in mind, with measures in place to protect user data and prevent unauthorised access. This includes using encryption, secure authentication mechanisms, and other security features.

- **Compatibility**: The Platform should be compatible with different devices and operating systems, and should work seamlessly with both iOS and Android devices.

- **Scalability**: The Platform should be designed to handle growth and increased usage over time. This includes using scalable architecture, such as cloud-based servers and databases, to ensure that the Platform can handle increasing traffic and usage.

- **Market Appearance**: The Platform architecture should be generic, ensuring that it could be easily adapted for other market applications.

The design process of the web collaborative platform focused on facilitating LEAs and Policy Makers ability to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The developed web collaborative platform helps to improve the efficiency of the communication between LEAs, Policy Makers and Citizens, with a particular focus on information sharing.

3. INTERACTION WITH OTHER WORK PACKAGES

Design and development of the PROACTIVE CBRNe Web collaborative platform for LEAs and security policy makers was predominantly the responsibility of WP4. Inputs for this work were provided from WP1, WP2, WP3, WP7 and WP8, determining the needs and gaps of the users in terms of current public perceptions relating to CBRNe incidents. The outcome of the research completed in WP1 contributed into the key engagement tasks in WP2, and by default, provided key feedback for the PROACTIVE Web Based platform in WP4. These interactions were laid out in D4.1 [1]:

Since the publication of D4.1 in March 2021, the following new interactions have occurred:

- Development and approval of the objective technical criteria for performance evaluation of the PROACTIVE Crisis Communication System with PROACTIVE consortium members during Progress Meetings;

- Multiple workshops with targeted end-users carried out as part of WP2 and WP3:
  - Online PSAB Workshop on 25 February 2021 (details are reported in Section 4.1);
  - Online CSAB Workshops on 26 February 2021 (Section 4.1);
  - Data Breach workshop on 4 March 2021 (details are reported in Section 4.2 & D8.2);

    - Online CSAB Focus Groups on 12 May, 26 May and June 2021 (Section 4.3);
    - The Joint CSAB-PSAB Workshop held in-person on 6 – 7 April 2022[1] (Section 4.5);
- Integration with the Mobile App for Vulnerable Citizens (WP5);
- Testing and verification of the PROACTIVE Crisis Communication System during the three field exercises organised as an integral part of WP6:
    - Contributions to the development of the Observer Guide questionnaire and its analysis.
    - Dedicated sessions during the Pre-Exercise Online Briefings to help Observers download and install the app.
    - Monitoring and analysing technical performance.
- Ensuring sustainability and market uptake of the Crisis Communication System in tandem with WP7;
- Participation and contribution to WP8 activities:
    - Involvement in the Social Impact Assessment and translating these recommendations into technical requirements for implementation in the PROACTIVE Communication System;
    - Evaluation of the Secure by Design concept and ensuring that PROACTIVE Communications System is compliant with these requirements.

Figure 1 below provides graphical illustration of the collaboration and interaction of WP4 with other WPs of PROACTIVE project.

[1] https://uic.org/com/enews/article/proactive-eu-project-holds-its-11th-consortium-meeting-and-a-joint-workshop

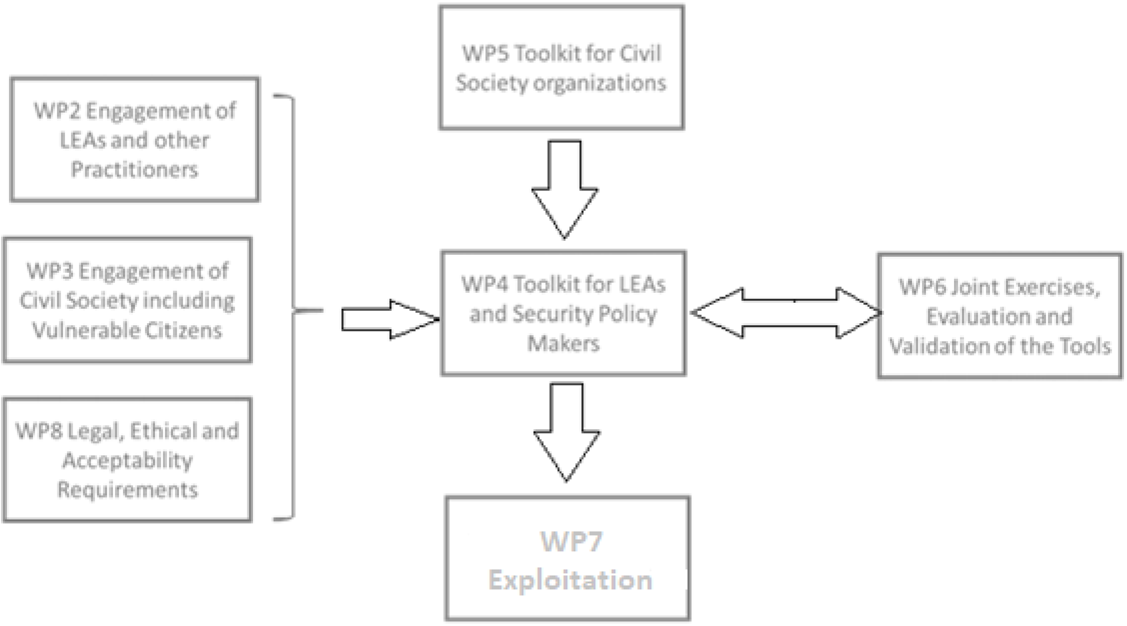

WP5 Toolkit for Civil Society organizations
WP2 Engagement of LEAs and other Practitioners
WP3 Engagement of Civil Society including Vulnerable Citizens
WP8 Legal, Ethical and Acceptability Requirements
WP4 Toolkit for LEAs and Security Policy Makers
WP6 Joint Exercises, Evaluation and Validation of the Tools
WP7 Exploitation

Figure 1 WP4 Collaboration and interaction with other WPs of PROACTIVE

Thanks to this iterative, co-creation process with many feedback loops and interactions with other WPs, at least 18 new versions of the PROACTIVE Crisis Communication System (made up of the Mobile App(s) and web collaborative platform) were released, which goes beyond the original amount of versions as laid out in the project Description of Action (DoA).

4. END USER REQUIREMENTS COLLECTED PRIOR TO THE FIELD EXERCISES

Based on the requirements set out in D4.1 & D5.3, the first prototype online web collaborative platform was developed and released for initial testing and verification by the PROACTIVE consortium. Following these tests, it was suggested to engage PSAB and the CSAB for further testing and advise from user perspective. It needs to be emphasised that this work was not originally planned in the original DoA. However, the benefits of such an evaluation were obvious so a decision was made to spend additional efforts on these extra tasks.

Even though this activity was not in the original DoA, the prototype was then tested with the PSAB & the CSAB during numerous workshops and focus groups organised by the UIC; details of the stakeholder engagement model are described in Havârneanu et al., 2022 [2]. However, Covid-19 pandemic affected all ways of life Globally and PROACTIVE project was not exempt from it. However, consortium members quickly adapted to a new reality and under the leadership of UIC new ways of project execution were introduced. One of the core components of this new approach was continued engagement with PROACTIVE stakeholders through online workshops and focus groups, organised by UIC, even though this was additional workload. One of the main challenges that needed to be overcome was to ensure that critical mass of practitioners and stakeholders will participate in the workshop in challenging conditions of Covid-19 pandemic. The project successfully recruited members from the advisory board to participate in all engagement activities.

Following the workshops, the PROACTIVE Crisis Communication System was redesigned, putting recommendations from the stakeholders as the key requirement (including the redesign of collaborative web platform and a first development of the Mobile App). Two additional factors contributed to this decision:

- PROACTIVE project extension due to Covid-19 pandemic.
- Iterative development process accepted by the PROACTIVE project.

The decision wasn't an easy one as it required a lot of additional work efforts which were not originally planned. This was complicated by the fact that RINISOFT lost a few development engineers who left the company and moved to other countries after Covid-19 pandemic. But all the additional efforts paid off as the new and revised version of the Crisis Communication System, developed based on direct specifications from the end users, eventually ensured successful use during the field exercises.

During the workshops and focus groups, feedback was collected and analysed using the Must have, Should have, Could have, and Won't have (MoSCoW) methodology and a refined set of requirements were laid out. MoSCoW is a prioritisation technique commonly used in project management and software development to classify requirements or features based on their importance and urgency. The MoSCoW prioritisation technique was first introduced by Dai Cleggin in 1994 [3]. He developed this approach while working on the Dynamic Systems Development Method (DSDM), an agile project management framework. MoSCoW became a fundamental aspect of DSDM and has since been widely adopted in various project management methodologies, including PROACTIVE, particularly in the field of software development. It provides a structured approach for prioritising requirements and making informed decisions about project scope and deliverables. Each category represents a different level of priority for the project or product being developed.

4.1. PSAB & CSAB Workshops Requirements

There were two consecutive workshops and the first workshop was conducted with 18 PSAB participants representing all categories of CBRNe practitioners on the 25 February 2021 [4]; and the second one involved 10 CSAB members representing mainly experts or researchers on the 26 February 2021 [5].

The workshops took the form of an incident-based discussion followed by a presentation of the web platform and then a live questionnaire. Participants were provided a fictitious CBRNe scenario, involving a suspected chemical attack set on a train carriage, and asked questions about their reactions to such situations. The live questionnaire asked questions specifically concerning the App functionality, design and accessibility. The incident-based discussion and live questionnaire allowed for the further elaboration of the requirements. First of all, we collected detailed feedback on the usefulness of existing features. These are shown in Table 1.

Table 1. Feedback on the existing features collected during the first workshop

Must have	Should have	Could have	Won't have
• Live alerts during an incident • Pre-Incident Information/ communication materials • Possibility to share information, including location and images	Contact details of LEAs and Vulnerable Citizen Organisations	Forum and/or Direct Messaging between LEAs and Citizens	Not applicable (N/A)

These workshops created foundation for closer engagement with PROACTIVE stakeholders and CBRNe practitioners. Further, these two workshops allowed us to collect new input, including additional features that the App must, should or could have. These are shown in Table 2. UIC, who organised the workshop, tried to keep interactive workshop format even though these workshops were organised online. To achieve this, live evaluation sessions were introduced and during these live evaluation sessions of the workshops, when asked to rate the web platform out of five stars, the PSAB workshop participants gave it 4 stars while the CSAB participants gave it 3. This symbolic exercise has demonstrated the importance of user engagement and was used to give an overall impression about the web platform quality perception within each group of users and provide a baseline for how the rating is going to change over time.

Table 2. Additional features collected during the workshops.

Must have	Should have	Could have	Won't have
• Better accessibility features, including: • Text-to-speech • Translation • Big text • Basic wording • Uncomplicated structure • Pictures, pictograms • Big buttons, icons and symbols • Colour blind mode for images/mapping • Specific information on what is happening and how to act	• Less text • Mental health support message • A symptoms checklist • Hospital lists • Links to other useful apps	• Social media integration (post information to a given social media account) • Ways to contact relatives/loved ones • Proof of decontamination	• Live camera feed to App for transmission to First Responders

4.2. Data Breach Workshop Requirements

Therefore, in addition to two workshop explained in the previous section, the PROACTIVE Data Breach Tabletop Exercise (TTX) took place on 4 March 2021 and had 10 participants, including security experts from law enforcement agencies and ethics experts. It was a scenario-based discussion in the format of a focus group. This workshop allowed for the development of requirements related to the prevention and mitigation of data breaches which are summarised in the Table 3 below. Full details of the data breach workshop were reported in D8.2 [6].

Table 3. Requirements related to the prevention and mitigation of data breaches

Must have	Should have	Could have	Won't have
• A means to secure the integrity and confidentiality of personal data • Anonymisation, pseudonymisation and encryption • A means to provide information about the potential source of the data breach and data subjects involved • The ability to communicate the breach to the supervisory authority based on data regulations and, in some cases, also the data subjects (the citizens) • The functionality to preserve the leak's circumstances, as preservation is a key aspect of digital forensics	• Ability to switch off the false data source • Ability to detect if the data breach is human error, misuse or an intentional attack • A tool within the App to rapidly report leaks to users • The protocol to be followed in case of data leaks	• Include a system to catalogue received information according to the source in some way; • A way to register logs to the system integrated into the platform • A data breach communication protocol	• Direct integration with other apps

4.3. Focus Groups with the CSAB

The discovered format of stakeholder engagement was well accepted by all the participants and a decision was made to enhance this programme until travel restrictions are removed. Therefore, three online Focus Groups with CSAB members were held in May-June 2021 in the following order:

- 12 May 2021 with 4 participants representing the blind/visually impaired, autistic, and mobility restricted;
- 26 May 2021 with 9 participants representing the blind/visually impaired, the deaf/hard of hearing, the LGBTQ-community, and the mobility restricted; and

- 8 June 2021 with 6 CSAB members representing the homeless, pregnant women, senior citizens, visually impaired guide dog users, and immigrants.

This format was selected deliberately as the goal was to separate the CSAB into smaller working groups and collect their inputs separately once they had a hands-on experience with the web platform during an incident-led discussion. Discussions within the focus groups concentrated on accessibility and ease-of-use of the app, which led to the following requirements (Table 4). Moreover, the focus groups gave the App a rating of 2.6 stars out of 5 on average. Detailed results are reported in Petersen et al., 2022 [5].

Table 4. Accessibility requirements collected during the 3 focus groups

Must have	Should have	Could have	Won't have
• Compliance with international standards for accessibility (e.g., WCAG 2.1) • Accessibility features, including: • Translation • Ability to zoom for the partially sighted • A high contrast option • Audio information • International Sign Language • An Easy Read mode A less chaotic interface	• A search button • Less confusing icons (e.g., contact icon should be an envelope, not an arrow) Less reliance on maps	N/A	N/A

4.4. Translation of MoSCoW findings into design and functional requirements

Let's go through each MoSCoW category in more detail. Once gathered, the MoSCoW findings were translated to PROACTIVE Crisis Communications System design and functional requirements, promoting the customisation elements needed to address the demands clearly explained during the workshops by each user group. This selected method ensured a core set of key functionalities are helped to build the overall system architecture ensuring a modular, flexible, scalable, robust and secure system is built. The architectural definition process focused on the following four principal objectives:

- To clearly present a description of the PROACTIVE system and how it addresses the stakeholder needs (including LEAs and vulnerable citizens);
- To provide a clear description of the critical aspects that need to be taken into consideration to ensure the system is modular, flexible, extensible, scalable, robust and secure;
- To provide enough details to allow technical teams to build instances of the system that share a common structure and consequently are interoperable by design;
- To ensure consistency for the MoSCoW findings by using this architecture design as a baseline input.

Concretely, this meant, for the MoSCoW requirement of “a less chaotic interface”, the collaborative web Platform homepage was redesigned to have a less complicated structure and a more ergonomic interface. For example, the “report an incident” button is now a standalone button, no longer under the heading of “get involved,” and has been coloured as a different colour (in this case red) and shade (lighter) than the other buttons to demonstrate its importance.

To meet the Must have requirement of better accessibility features, the web platform was updated to use larger font sizes, bigger buttons and bigger icons.

“The PROACTIVE Platform is your one-stop hub for all things Communication in relation to CBRNe incidents. The terms CBRNe refers to any Chemical, Biological, Radioactive, Nuclear and Explosive incidents and through the Platform you can:

- Report and receive live notifications about ongoing incidents in your area;
- Access pre-incident information on incidents;
- Interact with Law Enforcement Agencies and Civilian Organisations.”

Another example is that the contact icon was depicted as an arrow and has now been replaced with an envelope, the icon which the participants felt best depicted the idea of contact. Furthermore, the exclamation mark by share information made it seem that one would receive information and not report it to the police, so this was removed.

4.5. Release of the Mobile App at the Joint CSAB-PSAB Workshop in Paris

Up till April 2022, all engagement activities (workshops, focus groups) with the PROACTIVE Advisory Boards describe in the above sections and feedback sessions with PROACTIVE Consortium members during Progress Meetings were carried out using a prototype web collaborative platform.

Starting at the Joint CSAB-PSAB Workshop in Paris and continuing on to the three field exercises, end-user requirements were collected based on the Mobile App[2]. Indeed, all the end-user requirements collected regarding the prototype collaborative web platform were also applied to the mobile app, which debuted during the Joint CSAB-PSAB Workshop. However, it is important to note that just in the case of the requirements collected via testing of the web collaborative platform being applicable to the Mobile App, all requirements collected in regards to the Mobile App were also applied to the web collaborative platform.

A key example of this can be taken from the development of the now entitled CBRNe Library. Since its inception, one aspect of the PROACTIVE Crisis Communication System was to foster CBRNe incident preparedness through stocking relevant CBRNe preparedness materials (including but not limited to the PROACTIVE Pre-Incident Information Materials developed in D5.2 [7]) in a dedicated repository. In the original web collaborative platform prototype this area was called “CBRNe Information” and so was transferred as such to the Mobile App. During the Paris Workshop, it became clear that this was confusing to participants, with many thinking that if they clicked on the “CBRNe Information” button, they would find out information about the on-going CBRNe Incident. At the suggestion of the targeted end-users, the verbiage was changed to better reflect its actual purpose (that of a repository and not of informing about ongoing incidents): CBRNe Information became CBRNe Library. This change was not applied only to the Mobile App but was also applied to the web collaborative platform.

[2] Regarding the mobile app(s), while the DoA distinguishes between a Mobile App for Practitioners and a Mobile App for Vulnerable Citizens, this is in actuality the same app, differentiated by user groups (admin rights for Practitioners, and both a registered user and non-registered user for (vulnerable) citizens). See D4.3 & D5.4 for more.

5. SYSTEM DEVELOPMENT

5.1. General Approach

The PROACTIVE CBRNe Web Collaborative Platform was developed based on an iterative approach in line with the three field exercises completed during the lifetime of the PROACTIVE project. Numerous iterations of the developed system were implemented as a feedback loop for system optimisation as shown in below diagram.

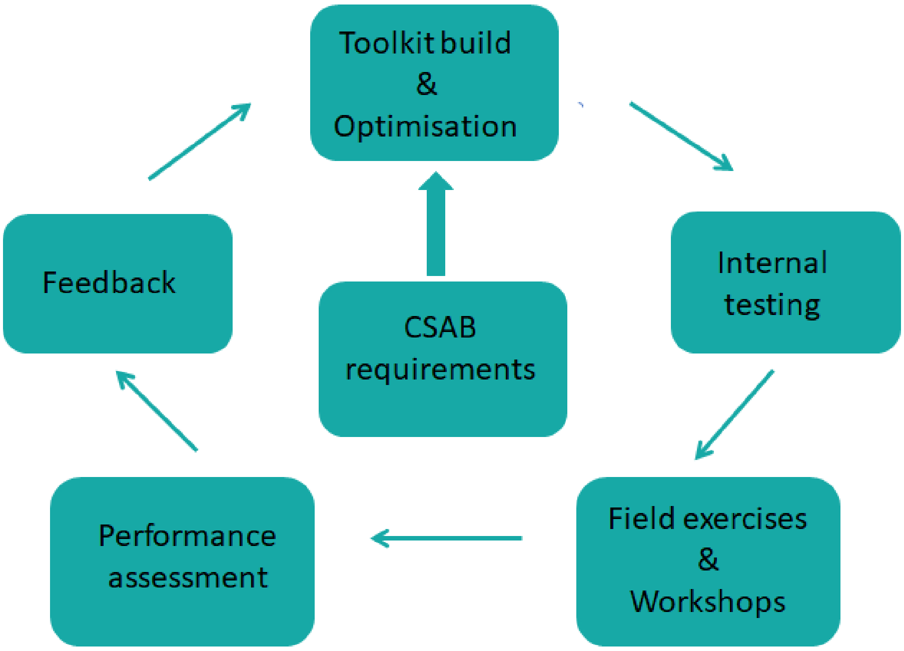


Figure 2 Iterative approach to web platform development

As it is shown on this figure, initially focus was placed on the CSAB requirements, then the PSAB and the final exercise will amalgamate the two. The final phase of the development was dedicated to incorporation of the currently available content, effectively showcasing the usability and purpose of the system during and post exercises, which produced recommendations for further optimisation, as an integral part of the overall iterative process.

5.2. PROACTIVE CBRNe Crisis Communication Systems Architecture

As mentioned earlier, the PROACTIVE CBRNe web collaborative platform is an integral part of the PROACTIVE CBRNe Crisis Communications System. Therefore, the development of the PROACTIVE CBRNe web collaborative platform commenced with the conceptual design of the overall communications system which is shown in figure below.

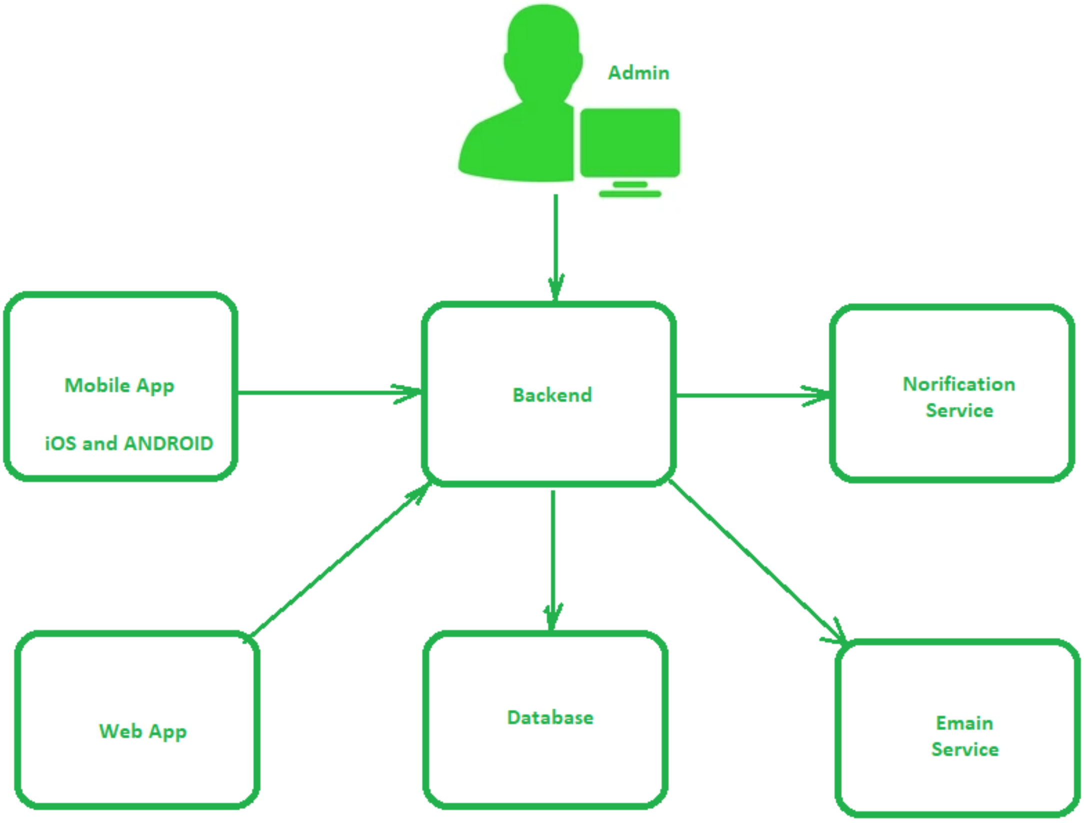


Figure 3 Block Diagram of the PROACTIVE CBRNe Crisis Communications System

As it follows from this diagram, in the core of the PROACTIVE CBRNe communications system is a dedicated platform ("Backend") which manages and coordinates the overall system. Developing such a communications system was a complex process that involved multiple iteration stages throughout the project duration and included planning, designing, developing, testing, and deploying.

In the core of our development were the following principles:

- ***User-centric design:*** The system was designed with the needs and preferences of the target audience in mind.
- ***Usability:*** The system was designed to be easy to use and navigate, with intuitive controls and clear instructions.

- ***Performance:*** The system was designed to be fast, responsive, and reliable, with minimal latency and downtime.
- ***Security:*** The system was designed with security in mind, with robust authentication and authorisation mechanisms, data encryption, and protection against common attack vectors.
- ***Scalability:*** The system was designed to be able to handle a growing user base and increasing traffic, without experiencing performance or functionality issues.

5.3. PROACTIVE CBRNe Collaborative Web Platform Architecture

The block diagram of the collaborative web platform is shown in Figure below.

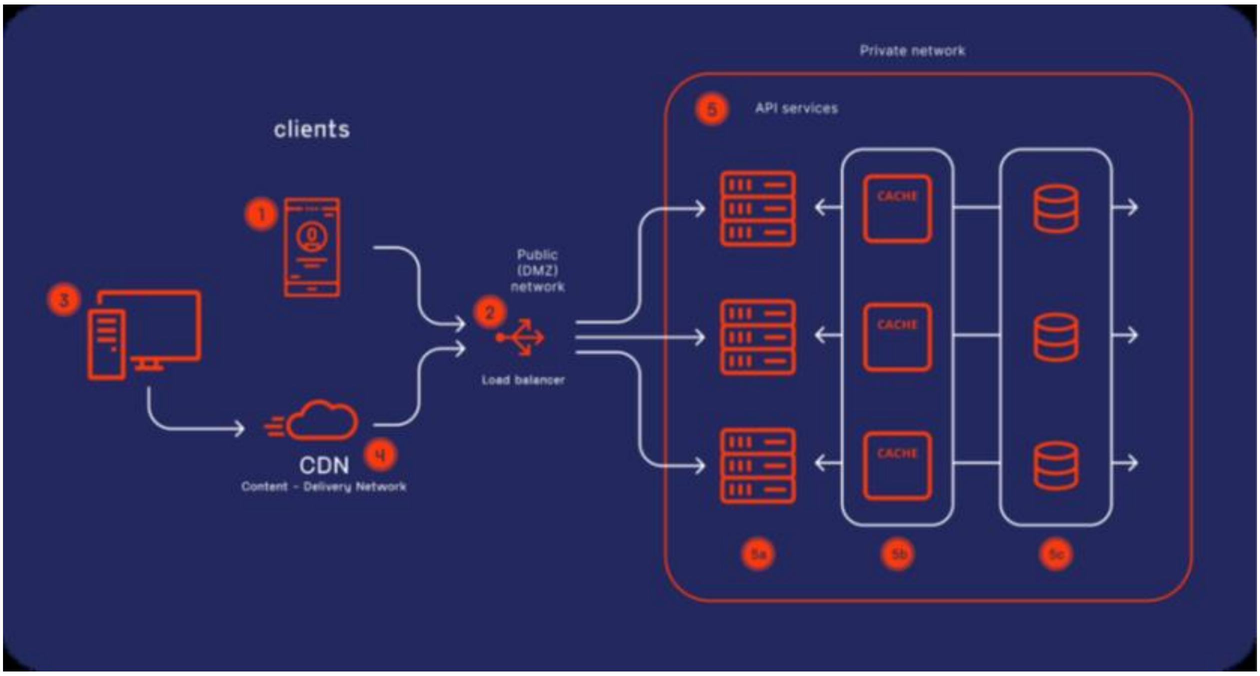


Figure 4 Block Diagram of the PROACTIVE CBRNe Communications Web Platform

As it follows from this diagram, the developed collaborative web platform manages and coordinates data flow between the stakeholders. When developing the CBRNe communications system in general and the collaborative web platform in particular, we envisaged the worse case scenario when no public communications infrastructure will be available during a CBRNe incident. In this scenario, no legacy communications platform which is relying on cellular or Wi-Fi connectivity can be used. Furthermore, all legacy tools which utilise existing social media apps (e.g. Facebook, WhatsApp or Telegram) also cannot be used as they require internet access to connect with the centralised server. Taking into account that the probability of no communications infrastructure during a CBRNe event is quite high (for example this happened during terrorist attacks in London, Paris, Brussels, when public communications infrastructure was switch off deliberately to avoid remotely controlled bomb explosions). Therefore, the developed platform is designed with unique feature to support reliable and robust operation of PROACTIVE CBRNe communications system over private and restricted networks, such as mesh networks established by the First Responders as an integral part of incident response. ***This feature makes the developed system unique in comparison with the possible***

existing solutions (WhatsApp, Facebook, etc), which require INTERNET connectivity for their operations.

5.4. CCS Functionality and Selected Development Tools

As explained in D4.1 [1] and earlier sections of this report, PROACTIVE CBRNe Crisis Communications System functionality was defined through a technical analysis of the user requirements supported by non functional requirements covering areas such as the legal, ethical, security, accessibility, scalability, usability and deployment. The system will be made up of two main components:

5.4.1. ASP.NET Core 3 Stateless Web Service

The desired system functionality was achieved through utilisation of the ASP.NET Core 3 a cross-platform for building modern web applications and services. ASP.NET Core 3 framework provides developers with the ability to build stateless web services. The stateless nature of the web service means that each client request is treated independently, without any reliance on previous requests or client-specific state. This simplifies the design and allows the service to handle a large number of concurrent requests without worrying about maintaining session state or shared resources. To ensure the required simplicity and user friendliness we utilsed modular architecture that allows developers to select only the necessary components for their application, resulting in improved performance and reduced overhead.

ASP.NET Core 3 provides extensive support for developing RESTful APIs, making it an ideal choice for building web services that follow the principles of the Representational State Transfer (REST) architectural style. It includes features such as attribute routing, content negotiation, model binding, and input validation, which help streamline the development of API endpoints and allows seamless integration of other platforms, as was requested in one of the core requirements.

Additionally, ASP.NET Core 3 offers robust security features to protect the web service and its resources. It supports various authentication and authorisation mechanisms, including JWT (JSON Web Tokens), OAuth, and OpenID Connect, allowing RINISOFT developers to implement secure access control for PROACTIVE collaborative web platform APIs.

Another reason why the ASP.NET Core 3 framework was selected for development – it provides seamless integration with popular data access frameworks, allowing RINISOFT developers to easily connect to databases and perform data operations within their stateless web service.

5.4.2. Angular 9 Reactive Web Application

To develop web applications for PROACTIVE CBRNe collaborative web platform, RINISOFT utilised Angular 9 open-source framework for building web applications with responsive and interactive user interfaces. In addition, RINISOFT applied reactive programming paradigm that focuses on asynchronous data streams and the propagation of changes.

Angular 9 is well suited for such a development and helped to meet both the functional and non-functional requirements defined during the stakeholder workshops, as explained earlier. It provides a comprehensive set of tools and features that make it easy to build reactive web applications.

Angular 9 also introduces a powerful form handling mechanism called Reactive Forms. Reactive Forms provide a reactive approach to working with forms, enabling developers to create dynamic and interactive form inputs with ease. Reactive Forms make it straightforward to perform form validation, handle user input, and reactively update the application state based on form changes. This feature is particularly important during a CBRNe incident when potentially large number of user inputs is expected to be received by the collaborative web platform at a very short time interval.

Furthermore, Angular 9 embraces a component-based architecture, which promotes code reusability and maintainability. By breaking the application into modular components, developers can build reusable UI elements and easily manage their state and behaviour. Again, taking into account commercialisation plans for the developed PROACTIVE Communications System this feature of Angular 9 is particular attractive as it will help to adapt the developed system for applications outside of CBRNe scenarios.

Figure 5 Linux Based Server shows the logical topology of an example single server deployment of the Proactive Application. The top half of the diagram shows the supported devices & web browsers (Safari, Firefox & Google Chrome), which allow the users to connect to the Server via a secure HTTPS connection. The bottom half of the diagram shows the connections & relationships between the installed components on the server:

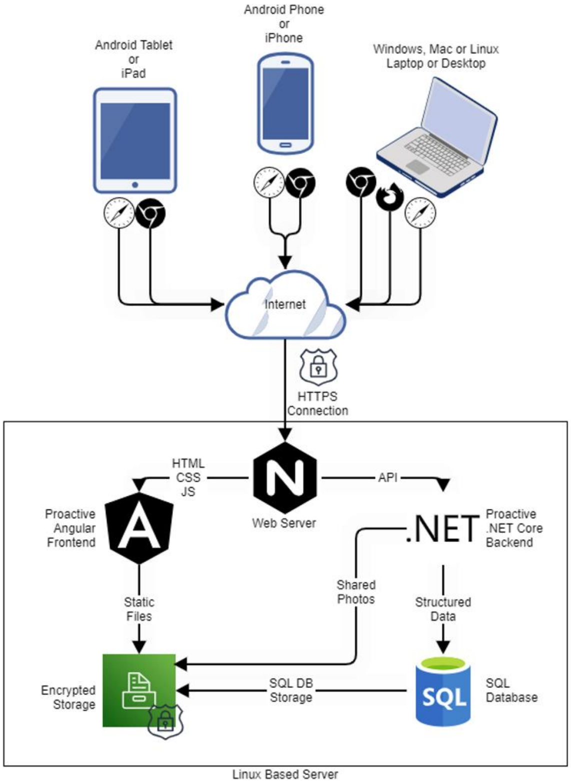


Figure 5 Linux Based Server

5.5. PROACTIVE CBRNe Collaborative Web Platform Security

The PROACTIVE CBRNe collaborative web Platform is designed to be compliant with the concept of “Secure by Design”. The main principles of this concept are outlined in the Table below:

Table 5. Main Principle of Secure by Design

Principle	Implementation
Minimising attack surface:	This principle involves reducing the opportunities for attackers to exploit vulnerabilities in a system by reducing its attack surface. This can be achieved by implementing only necessary functionality and limiting access to sensitive data.
Layered defence:	This principle involves implementing multiple layers of defence to provide a more robust security posture. This can be achieved by using a combination of security controls such as firewalls, intrusion detection systems, and encryption.
Principle of least privilege:	This principle involves giving users and processes only the minimum level of access necessary to perform their tasks. This can help reduce the risk of unauthorised access and limit the potential damage that can be caused by a compromised account.
Secure default settings:	This principle involves implementing secure default settings for all systems and applications. This includes ensuring that all passwords are strong and not easily guessable, and that all default configurations are secure.
Fail-safe defaults:	This principle involves ensuring that systems and applications fail safely in the event of an error or security breach. This can help prevent attackers from exploiting vulnerabilities to gain unauthorised access or cause damage.

As an integral part of this approach, the developed web Platform incorporates the following security protocols:

- SQL Data Protected by Full Drive Encryption: aes-xts 256;
- Client-Server communication protected by Transport Layer Security (HTTPS);
- System access is controlled by application-level authorisation. Unauthorised users (not logged in) and members of the public may not view sensitive information or edit publicly accessible information directly. In addition, API Key authorisation will be available for external integrations.

The whole concept was verified by utilising “Secure by Design” verification platform developed by HORIZON project PANACEA[3].

5.6. PROACTIVE CBRNe Crisis Communications System Interoperability

Another unique feature of the developed PROACTIVE CBRNe Crisis Communications System is interoperability with the existing legacy systems. Furthermore, the developed communications system is designed as future proved, allowing integration of systems which could be introduced in the future. This is feasible because:

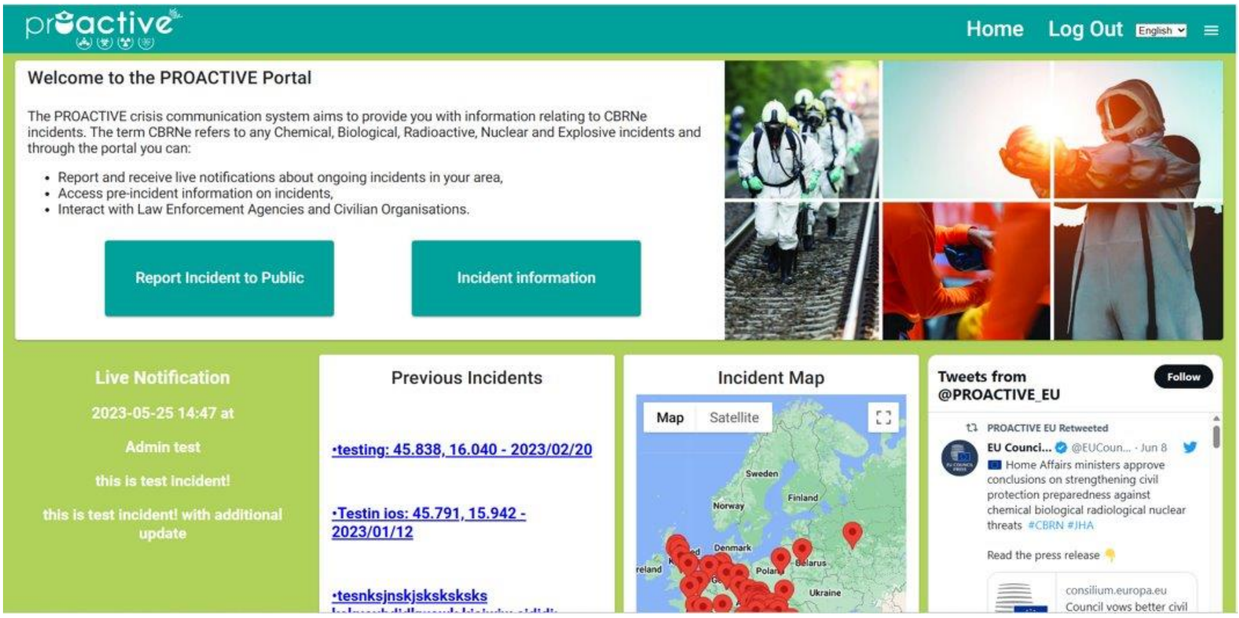
- The PROACTIVE platform exposes a secure REST API that allows for external systems to integrate;
- The integration API can be used by authorised partners to push data into the system in real time;
- The home page has links to external applications and resources.

This interoperability was tested during the last field exercise where PROACTIVE CBRNe communications system was linked and integrated with Twitter and LinkedIn social media platforms.

5.6.1. Graphic User Interface

The PROACTIVE Platform’s GUI is an Angular 9 Reactive web application that provides users with an accessible user interface to carry out the main functional interactions required of the PROACTIVE platform. The GUI is designed to cater for a diverse range of users and devices, and evolved through a number of changes and iterations which were generated as a response to suggestions from all the stakeholders. As most of the web app of the similar complexity, PROACTIVE CBRNe collaborative platform has a few pages each of which provide relevant information. The final version of the main page is shown in Figure below:

[3] https://cordis.europa.eu/project/id/826293



Welcome to the PROACTIVE Portal

The PROACTIVE crisis communication system aims to provide you with information relating to CBRNe incidents. The term CBRNe refers to any Chemical, Biological, Radioactive, Nuclear and Explosive incidents and through the portal you can:

- Report and receive live notifications about ongoing incidents in your area,
- Access pre-incident information on incidents,
- Interact with Law Enforcement Agencies and Civilian Organisations.

Live Notification

2023-05-25 14:47 at

Admin test

this is test incident!

this is test incident! with additional update

Previous Incidents

•testing: 45.838, 16.040 - 2023/02/20

•Testin ios: 45.791, 15.942 - 2023/01/12

•tesnksjnskjsksksksks

Incident Map

Tweets from @PROACTIVE_EU

PROACTIVE EU Retweeted

EU Counci... @EUCoun... · Jun 8

Home Affairs ministers approve conclusions on strengthening civil protection preparedness against chemical biological radiological nuclear threats #CBRN #JHA

Read the press release

consilium.europa.eu
Council vows better civil

Figure 6 PROACTIVE CBRNe Communications Web Platform Screenshot

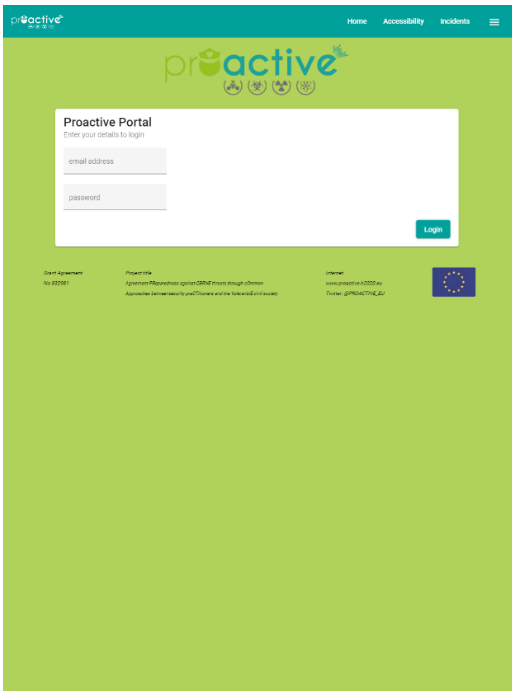
As requested in initial requirements, the developed PROACTIVE CBRNe web platform GUI supports:

- Landscape and Portrait aspect ratios;
- Screen sizes from 10cm to 50+cm;
- iOS phones and tablets;
- Android phones and tables;
- Laptop & Desktop browsers; Chrome, Firefox, Edge, Opera and more;
- Screen readers & accessibility tools;
- Progressive Web App to provide offline functionality and asynchronous file uploads.

The homepage acts as the central hub for the technology, enabling users to navigate to the relevant areas of interest. This page also acts as a main notification page, providing users with live updates either directly through the PROACTIVE Mobile Application or through link to national systems and news channels.

5.6.2. PROACTIVE Collaborative Platform Login Page

This page allows registered users and site admins (LEAs) to log into the Platform and access application features not available to unregistered users. Screenshot of the login page is shown in figure below.



Proactive Portal

Enter your details to login

email address

password

Grant Agreement

No 832981

Project title

Agreement PReparedness against CBRNE threats through cOmmon Approaches betweensecurity praCTitioners and the VulnerablE civil society

Internet

www.proactive-h2020.eu

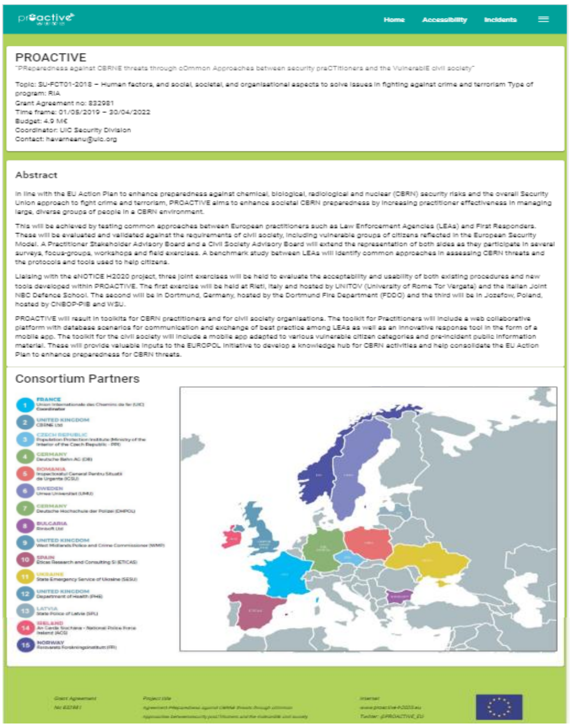
Twitter: @PROACTIVE_EU

Figure 7 Registration Page

It is not however mandatory to login to the Platform, information on CBRNe issues will be available without registering. Should users require further details they will have the option of requesting further information through the PROACTIVE email or via the website.

5.6.3. PROACTIVE Platform “About Us” Page

This is the page on Platform which doesn’t require login to the Platform as it provides project information for members of the public. The screenshot of this page is shown below:



PROACTIVE

"PReparedness against CBRNE threats through cOmmon Approaches between security praCTitioners and the VulnerablE civil society"

Topic: SU-FCT01-2018 – Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism Type of program: RIA
Grant Agreement no: 832981
Time frame: 01/05/2019 – 30/04/2022
Budget: 4.9 M€
Coordinator: UIC Security Division
Contact: havarneanu@uic.org

Abstract

In line with the EU Action Plan to enhance preparedness against chemical, biological, radiological and nuclear (CBRN) security risks and the overall Security Union approach to fight crime and terrorism, PROACTIVE aims to enhance societal CBRN preparedness by increasing practitioner effectiveness in managing large, diverse groups of people in a CBRN environment.

This will be achieved by testing common approaches between European practitioners such as Law Enforcement Agencies (LEAs) and First Responders. These will be evaluated and validated against the requirements of civil society, including vulnerable groups of citizens reflected in the European Security Model. A Practitioner Stakeholder Advisory Board and a Civil Society Advisory Board will extend the representation of both sides as they participate in several surveys, focus-groups, workshops and field exercises. A benchmark study between LEAs will identify common approaches in assessing CBRN threats and the protocols and tools used to help citizens.

Liaising with the eNOTICE H2020 project, three joint exercises will be held to evaluate the acceptability and usability of both existing procedures and new tools developed within PROACTIVE. The first exercise will be held at Rieti, Italy and hosted by UNITOV (University of Rome Tor Vergata) and the Italian Joint NBC Defence School. The second will be in Dortmund, Germany, hosted by the Dortmund Fire Department (FDDO) and the third will be in Jozefow, Poland, hosted by CNBOP-PIB and WSU.

PROACTIVE will result in toolkits for CBRN practitioners and for civil society organisations. The toolkit for Practitioners will include a web collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a mobile app. The toolkit for the civil society will include a mobile app adapted to various vulnerable citizen categories and pre-incident public information material. These will provide valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRN activities and help consolidate the EU Action Plan to enhance preparedness for CBRN threats.

Consortium Partners

1	FRANCE Union Internationale des Chemins de fer (UIC) Coordinator
2	UNITED KINGDOM CBRNE Ltd
3	CZECH REPUBLIC Population Protection Institute (Ministry of the Interior of the Czech Republic - PPI)
4	GERMANY Deutsche Bahn AG (DB)
5	ROMANIA Inspectoratul General Pentru Situatii de Urgenta (IGSU)
6	SWEDEN Umea Universitet (UMU)
7	GERMANY Deutsche Hochschule der Polizei (DHPOL)
8	BULGARIA Rinisoft Ltd
9	UNITED KINGDOM West Midlands Police and Crime Commissioner (WMP)
10	SPAIN Eticas Research and Consulting Sl (ETICAS)
11	UKRAINE State Emergency Service of Ukraine (SESU)
12	UNITED KINGDOM Department of Health (PHE)
13	LATVIA State Police of Latvia (SPL)
14	IRELAND An Garda Siochana - National Police Force Ireland (AGS)
15	NORWAY Forsvarets Forskningsinstitutt (FFI)

Grant Agreement
No 832981

Project title
Agreement PReparedness against CBRNE threats through cOmmon
Approaches between security praCTitioners and the VulnerablE civil society

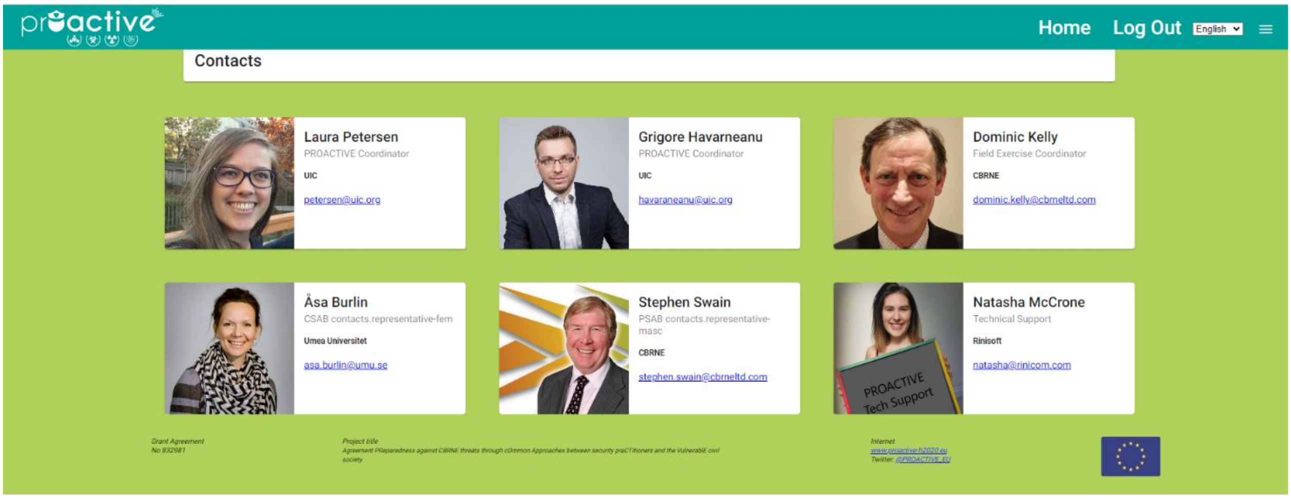
Internet
www.proactive-h2020.eu
Twitter: @PROACTIVE_EU

Figure 8 Screenshot of the "About Us" Page

The "About Us" page describes the project and its purpose and lists details the grant agreement information in addition to the purpose of the project.

5.6.4. Contacts Page

The contact page provides list of contacts from various PROACTIVE partner companies/institutions allowing a user to engage with PROACTIVE partners on various topics of interest. A screenshot of PROACTIVE CBRNe collaborative web Platform "Contacts" page is shown below



Contacts

Laura Petersen
PROACTIVE Coordinator
UIC
petersen@uic.org

Grigore Havarneanu
PROACTIVE Coordinator
UIC
havarneanu@uic.org

Dominic Kelly
Field Exercise Coordinator
CBRNE
dominic.kelly@cbrneltd.com

Åsa Burlin
CSAB contacts.representative-fem
Umea Universitet
asa.burlin@umu.se

Stephen Swain
PSAB contacts.representative-masc
CBRNE
stephen.swain@cbrneltd.com

Natasha McCrone
Technical Support
Rinisoft
natasha@rinicom.com

Grant Agreement
No 832981

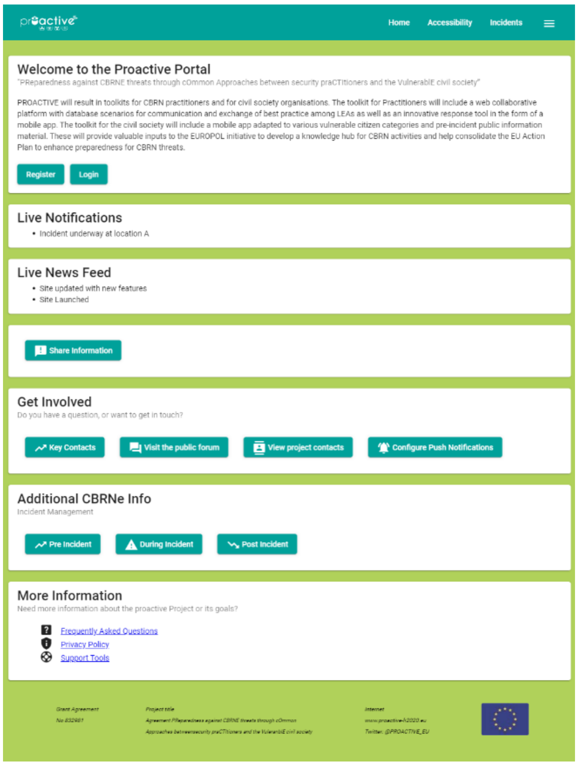
Project title
Agreement PReparedness against CBRNE threats through cOmmon Approaches between security praCTitioners and the VulnerablE civil society

Internet
www.proactive-h2020.eu
Twitter: @PROACTIVE_EU

Figure 9 Screenshot of PROACTIVE Collaborative Web Platform "Contacts" Page

5.6.5. Earlier Versions of Platform Home Page and Key Contacts

As mentioned in earlier sections, PROACTIVE CBRNe Communications Systems in general and collaborative web Platform in particular have undergone a number of interactions. This was done in response to various recommendations from different stakeholder groups and as a result of dedicated workshops. Even though this created additional workload, it was worthy as it helped to converge on the final version which performed well during the field exercises and was accepted by the users. The degree of transformations could be seen by comparing figure below (which was original landing page) with figure 6 which is the final landing page released as part of D4.2



Welcome to the Proactive Portal

"PReparedness against CBRNE threats through cOmmon Approaches between security praCTItioners and the VulnerablE civil society"

PROACTIVE will result in toolkits for CBRN practitioners and for civil society organisations. The toolkit for Practitioners will include a web collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a mobile app. The toolkit for the civil society will include a mobile app adapted to various vulnerable citizen categories and pre-incident public information material. These will provide valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRN activities and help consolidate the EU Action Plan to enhance preparedness for CBRN threats.

Live Notifications

- Incident underway at location A

Live News Feed

- Site updated with new features
- Site Launched

Get Involved

Do you have a question, or want to get in touch?

Additional CBRNe Info

Incident Management

More Information

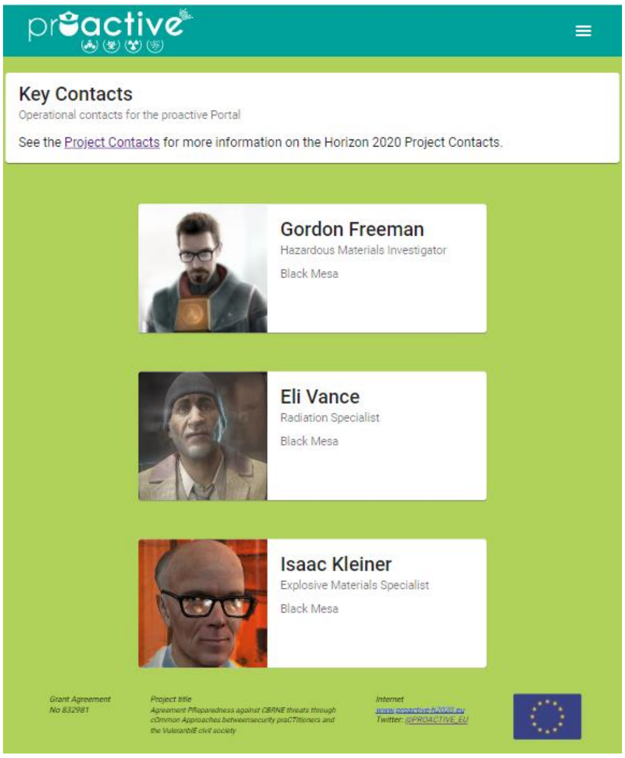
Need more information about the proactive Project or its goals?

- Frequently Asked Questions
- Privacy Policy
- Support Tools

Grant Agreement No 832981

Project title Agreement PReparedness against CBRNE threats through cOmmon Approaches betweensecurity praCTitioners and the VulerabIE civil society

Internet www.proactive-h2020.eu Twitter: @PROACTIVE_EU



Key Contacts

Operational contacts for the proactive Portal

See the Project Contacts for more information on the Horizon 2020 Project Contacts.

Gordon Freeman
Hazardous Materials Investigator
Black Mesa

Eli Vance
Radiation Specialist
Black Mesa

Isaac Kleiner
Explosive Materials Specialist
Black Mesa

Grant Agreement No 832981

Project title Agreement PReparedness against CBRNE threats through cOmmon Approaches betweensecurity praCTitioners and the VuleranbIE civil society

Internet www.proactive-h2020.eu Twitter: @PROACTIVE_EU

Figure 10 Initial Home Page and Key Contacts

5.6.6. Information Sharing

Live updated map of current incidents along with a summary of incident status. Registered users will have the capability to notify of an incident in their area. Basic details including date logged, the status and type of incident will be required in addition to the location. All incidents will be moved to a holding queue, in which LEAs will have direct access to the review and verify the incident. Once validated the LEA can then choose to release an update on the incident utilising the map functionality available in the Mobile Applications. Furthermore, LEAs will have the option to monitor and update the incident using the live notifications functionality once the incident has been investigated. Figures bellow include screenshots illustrating information sharing. More specifically, Figure below shows map with all reported incidents.

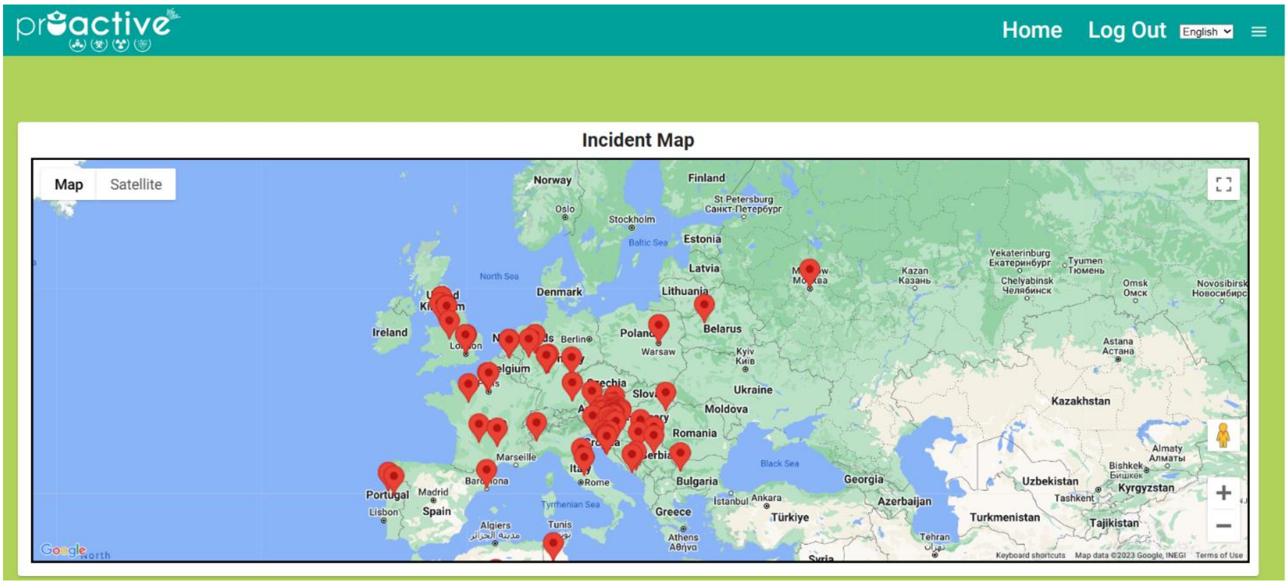
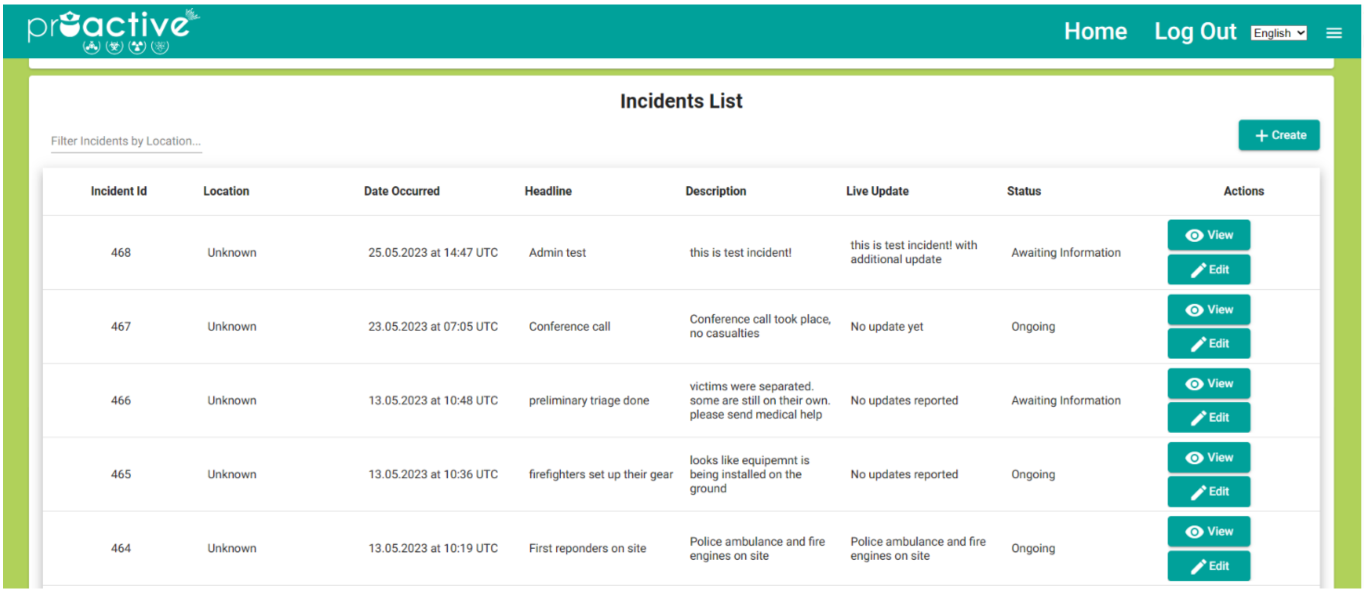


Figure 11 Map with the reported incidents

Is requested in original requirements, the map is scalable and is capable of showing the whole of Europe as well as the dedicated area with particular CBRNe incident.

Figure 12 shows a screenshot with all incidents reported by public. Each of these reported incidents includes detailed description, location coordinates and supporting audio/video data which help LEAs to classify the incident and decide about the next steps for dealing with it.

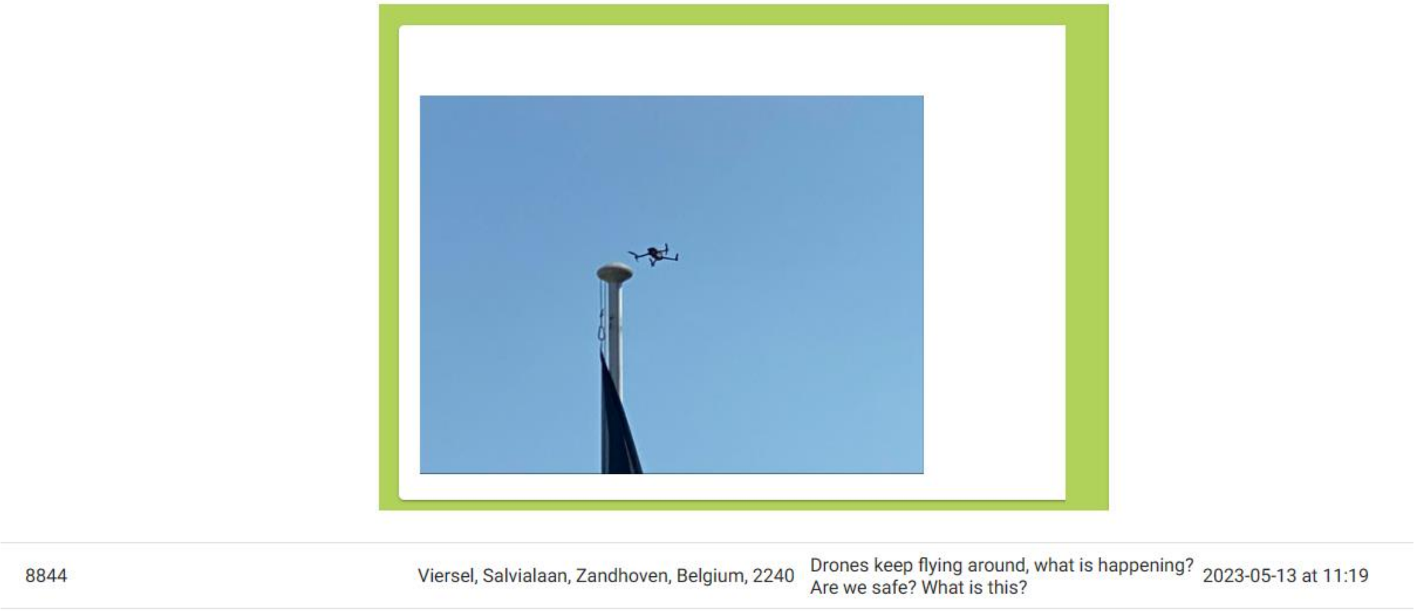


Incidents List

Incident Id	Location	Date Occurred	Headline	Description	Live Update	Status	Actions
468	Unknown	25.05.2023 at 14:47 UTC	Admin test	this is test incident!	this is test incident! with additional update	Awaiting Information	View Edit
467	Unknown	23.05.2023 at 07:05 UTC	Conference call	Conference call took place, no casualties	No update yet	Ongoing	View Edit
466	Unknown	13.05.2023 at 10:48 UTC	preliminary triage done	victims were separated. some are still on their own. please send medical help	No updates reported	Awaiting Information	View Edit
465	Unknown	13.05.2023 at 10:36 UTC	firefighters set up their gear	looks like equipemnt is being installed on the ground	No updates reported	Ongoing	View Edit
464	Unknown	13.05.2023 at 10:19 UTC	First reponders on site	Police ambulance and fire engines on site	Police ambulance and fire engines on site	Ongoing	View Edit

Figure 12 Incidents Reported by General Public

Figure 13 as an illustration, shows screenshot of video material with detected drone at the location of the third PROACTIVE exercise.

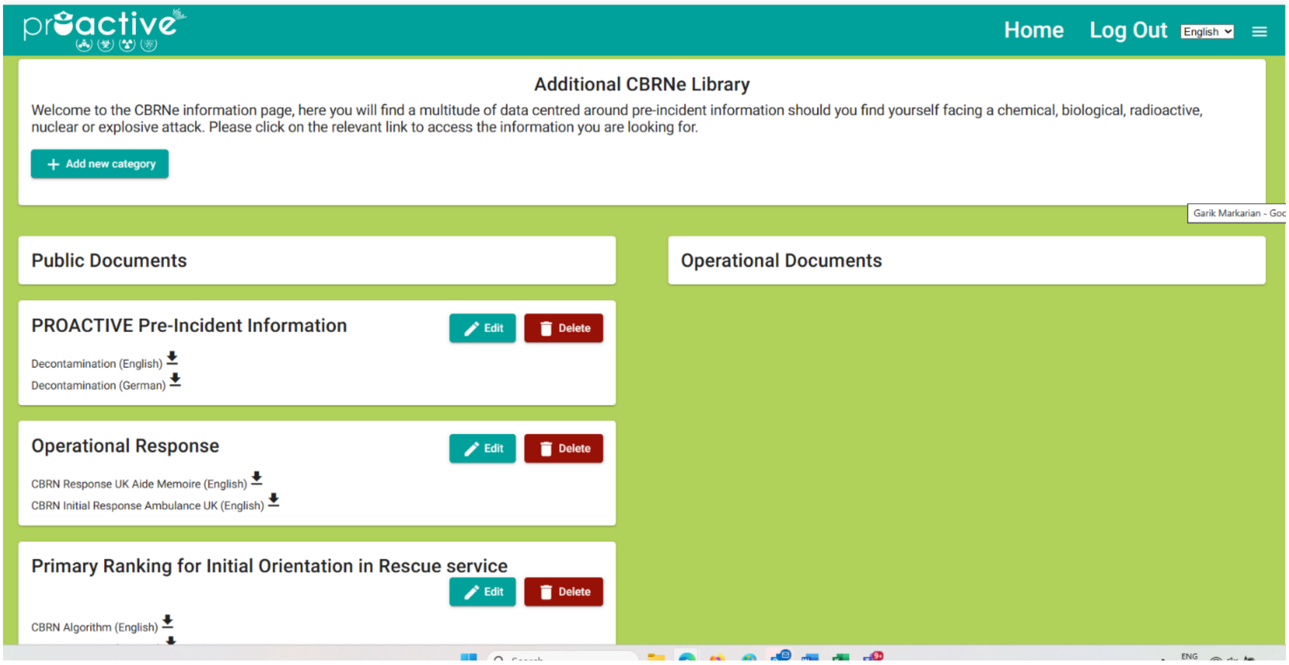


8844	Viersel, Salvialaan, Zandhoven, Belgium, 2240	Drones keep flying around, what is happening? Are we safe? What is this?	2023-05-13 at 11:19

Figure 13 Screenshot of one of the reports during the third PROACTIVE exercise

5.6.7. PROACTIVE CBRNe Library

One of the unique features of the developed PROACTIVE CBRNe communications system is a dedicated PROACTIVE CBRNe library, which was developed in close cooperation with all stakeholders and includes comprehensive information covering pre-CBRNe, during-CBRNe and post-CBRNe scenarios. Figure 14 bellow shows a screenshot of the PROACTIVE CBRNe Library page on the collaborative web platform while the next two figures (15 & 16) illustrate types of documents that are available for download by platform users.



Additional CBRNe Library

Welcome to the CBRNe information page, here you will find a multitude of data centred around pre-incident information should you find yourself facing a chemical, biological, radioactive, nuclear or explosive attack. Please click on the relevant link to access the information you are looking for.

Public Documents

Operational Documents

PROACTIVE Pre-Incident Information

Decontamination (English)
Decontamination (German)

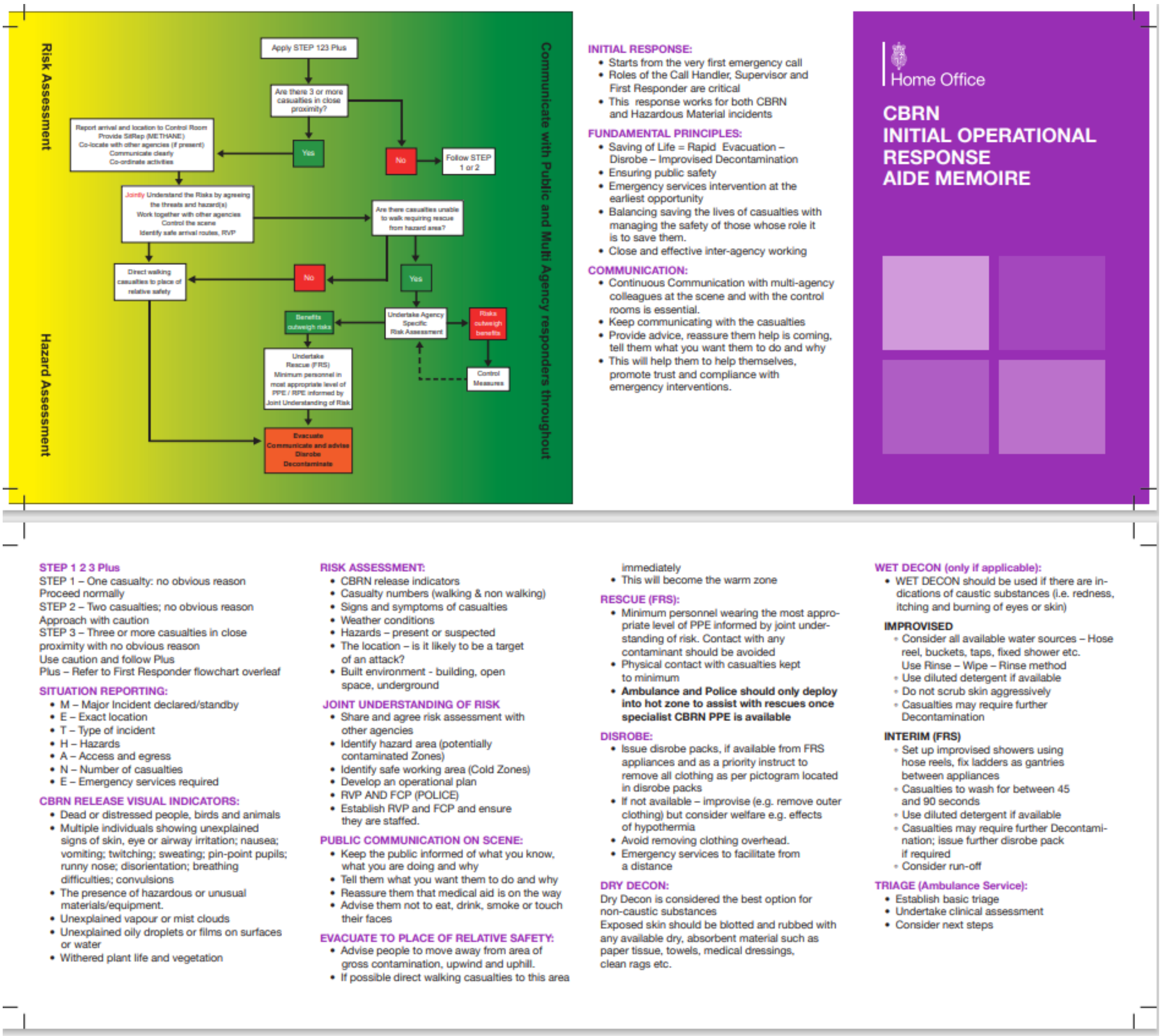
Operational Response

CBRN Response UK Aide Memoire (English)
CBRN Initial Response Ambulance UK (English)

Primary Ranking for Initial Orientation in Rescue service

CBRN Algorithm (English)

Figure 14 Screenshot of the page dedicated to CBRNe Library



Risk Assessment

Hazard Assessment

Apply STEP 123 Plus

Are there 3 or more casualties in close proximity?

Yes

No

Follow STEP 1 or 2

Report arrival and location to Control Room
Provide SitRep (METHANE)
Co-locate with other agencies (if present)
Communicate clearly
Co-ordinate activities

Jointly Understand the Risks by agreeing the threats and hazard(s)
Work together with other agencies
Control the scene
Identify safe arrival routes, RVP

Are there casualties unable to walk requiring rescue from hazard area?

No

Yes

Direct walking casualties to place of relative safety

Undertake Agency Specific Risk Assessment

Benefits outweigh risks

Risks outweigh benefits

Control Measures

Undertake Rescue (FRS)
Minimum personnel in most appropriate level of PPE / RPE informed by Joint Understanding of Risk

Evacuate
Communicate and advise
Disrobe
Decontaminate

Communicate with Public and Multi Agency responders throughout

INITIAL RESPONSE:

- Starts from the very first emergency call
- Roles of the Call Handler, Supervisor and First Responder are critical
- This response works for both CBRN and Hazardous Material incidents

FUNDAMENTAL PRINCIPLES:

- Saving of Life = Rapid Evacuation – Disrobe – Improvised Decontamination
- Ensuring public safety
- Emergency services intervention at the earliest opportunity
- Balancing saving the lives of casualties with managing the safety of those whose role it is to save them.
- Close and effective inter-agency working

COMMUNICATION:

- Continuous Communication with multi-agency colleagues at the scene and with the control rooms is essential.
- Keep communicating with the casualties
- Provide advice, reassure them help is coming, tell them what you want them to do and why
- This will help them to help themselves, promote trust and compliance with emergency interventions.

Home Office

CBRN
INITIAL OPERATIONAL RESPONSE
AIDE MEMOIRE

STEP 1 2 3 Plus

STEP 1 – One casualty: no obvious reason
Proceed normally
STEP 2 – Two casualties; no obvious reason
Approach with caution
STEP 3 – Three or more casualties in close proximity with no obvious reason
Use caution and follow Plus
Plus – Refer to First Responder flowchart overleaf

SITUATION REPORTING:

- M – Major Incident declared/standby
- E – Exact location
- T – Type of incident
- H – Hazards
- A – Access and egress
- N – Number of casualties
- E – Emergency services required

CBRN RELEASE VISUAL INDICATORS:

- Dead or distressed people, birds and animals
- Multiple individuals showing unexplained signs of skin, eye or airway irritation; nausea; vomiting; twitching; sweating; pin-point pupils; runny nose; disorientation; breathing difficulties; convulsions
- The presence of hazardous or unusual materials/equipment.
- Unexplained vapour or mist clouds
- Unexplained oily droplets or films on surfaces or water
- Withered plant life and vegetation

RISK ASSESSMENT:

- CBRN release indicators
- Casualty numbers (walking & non walking)
- Signs and symptoms of casualties
- Weather conditions
- Hazards – present or suspected
- The location – is it likely to be a target of an attack?
- Built environment - building, open space, underground

JOINT UNDERSTANDING OF RISK

- Share and agree risk assessment with other agencies
- Identify hazard area (potentially contaminated Zones)
- Identify safe working area (Cold Zones)
- Develop an operational plan
- RVP AND FCP (POLICE)
- Establish RVP and FCP and ensure they are staffed.

PUBLIC COMMUNICATION ON SCENE:

- Keep the public informed of what you know, what you are doing and why
- Tell them what you want them to do and why
- Reassure them that medical aid is on the way
- Advise them not to eat, drink, smoke or touch their faces

EVACUATE TO PLACE OF RELATIVE SAFETY:

- Advise people to move away from area of gross contamination, upwind and uphill.
- If possible direct walking casualties to this area immediately
- This will become the warm zone

RESCUE (FRS):

- Minimum personnel wearing the most appropriate level of PPE informed by joint understanding of risk. Contact with any contaminant should be avoided
- Physical contact with casualties kept to minimum
- **Ambulance and Police should only deploy into hot zone to assist with rescues once specialist CBRN PPE is available**

DISROBE:

- Issue disrobe packs, if available from FRS appliances and as a priority instruct to remove all clothing as per pictogram located in disrobe packs
- If not available – improvise (e.g. remove outer clothing) but consider welfare e.g. effects of hypothermia
- Avoid removing clothing overhead.
- Emergency services to facilitate from a distance

DRY DECON:

Dry Decon is considered the best option for non-caustic substances
Exposed skin should be blotted and rubbed with any available dry, absorbent material such as paper tissue, towels, medical dressings, clean rags etc.

WET DECON (only if applicable):

- WET DECON should be used if there are indications of caustic substances (i.e. redness, itching and burning of eyes or skin)

IMPROVISED

- Consider all available water sources – Hose reel, buckets, taps, fixed shower etc.
  Use Rinse – Wipe – Rinse method
- Use diluted detergent if available
- Do not scrub skin aggressively
- Casualties may require further Decontamination

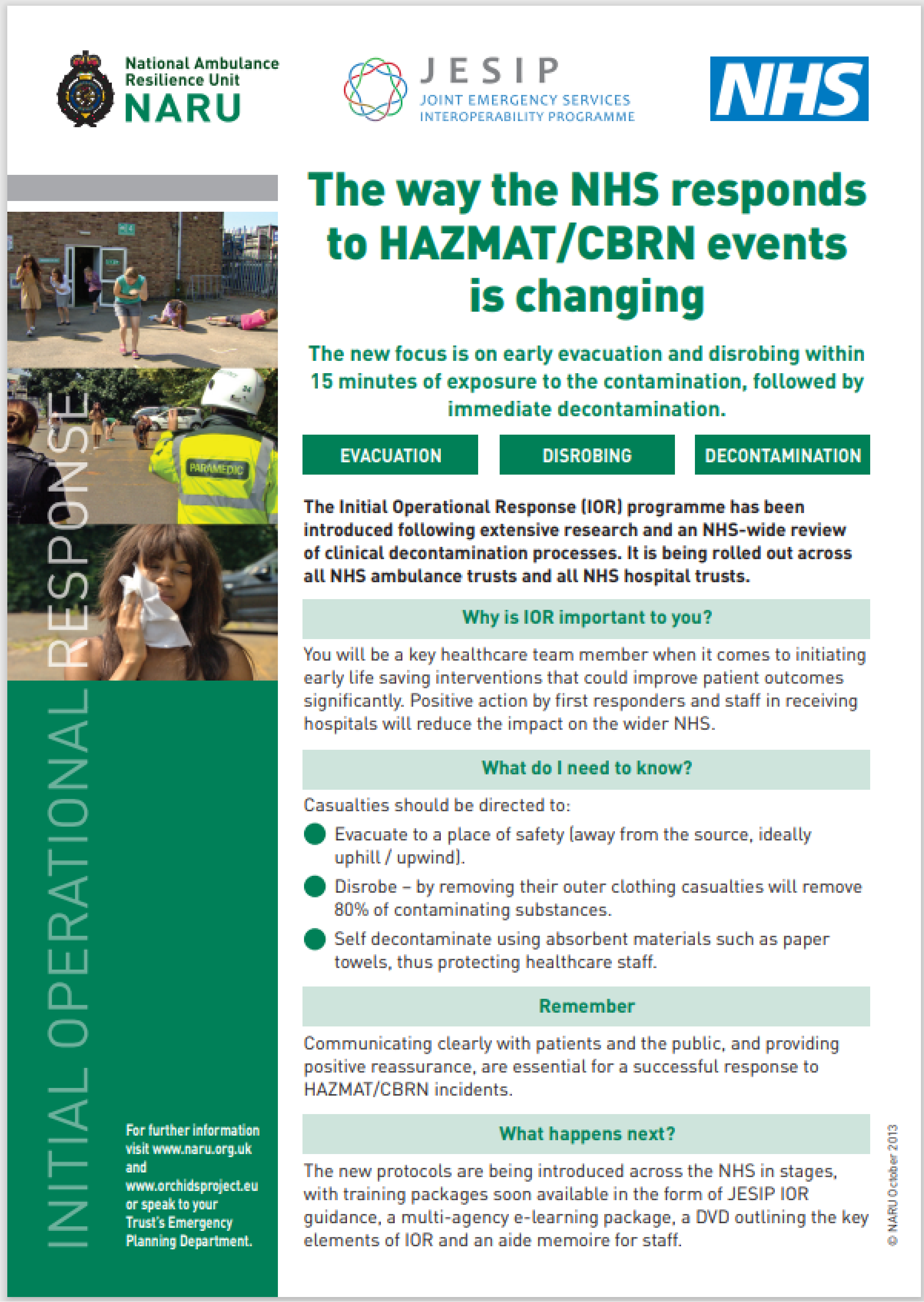
INTERIM (FRS)

- Set up improvised showers using hose reels, fix ladders as gantries between appliances
- Casualties to wash for between 45 and 90 seconds
- Use diluted detergent if available
- Casualties may require further Decontamination; issue further disrobe pack if required
- Consider run-off

TRIAGE (Ambulance Service):

- Establish basic triage
- Undertake clinical assessment
- Consider next steps

Figure 15 UK Home Office Document on PROACTIVE Collaborative Web Platform



National Ambulance Resilience Unit NARU

JESIP JOINT EMERGENCY SERVICES INTEROPERABILITY PROGRAMME

NHS

INITIAL OPERATIONAL RESPONSE

The way the NHS responds to HAZMAT/CBRN events is changing

The new focus is on early evacuation and disrobing within 15 minutes of exposure to the contamination, followed by immediate decontamination.

EVACUATION | DISROBING | DECONTAMINATION

The Initial Operational Response (IOR) programme has been introduced following extensive research and an NHS-wide review of clinical decontamination processes. It is being rolled out across all NHS ambulance trusts and all NHS hospital trusts.

Why is IOR important to you?

You will be a key healthcare team member when it comes to initiating early life saving interventions that could improve patient outcomes significantly. Positive action by first responders and staff in receiving hospitals will reduce the impact on the wider NHS.

What do I need to know?

Casualties should be directed to:

- Evacuate to a place of safety (away from the source, ideally uphill / upwind).
- Disrobe – by removing their outer clothing casualties will remove 80% of contaminating substances.
- Self decontaminate using absorbent materials such as paper towels, thus protecting healthcare staff.

Remember

Communicating clearly with patients and the public, and providing positive reassurance, are essential for a successful response to HAZMAT/CBRN incidents.

What happens next?

The new protocols are being introduced across the NHS in stages, with training packages soon available in the form of JESIP IOR guidance, a multi-agency e-learning package, a DVD outlining the key elements of IOR and an aide memoire for staff.

For further information visit www.naru.org.uk and www.orchidsproject.eu or speak to your Trust's Emergency Planning Department.

Figure 16 UK NHS Document of PROACTIVE Collaborative Web Platform

6. WEB PLATFORM VERIFICATION DURING THE FIELD EXERCISES

6.1. Verification Requirements

Verification and testing of any software is a key component of development and PROACTIVE CBRNe Communications web platform wasn't exempted from this process. Furthermore, as was requested in the original requirements, the developed web platform has undergone 2 independent verifications:

- Objective (technical) verification, which included testing, debugging and collection of objective measurable evidence after every PROACTIVE exercise;
- Subjective (user) verification through questionnaire, representing subjective expert views reflecting personal experience of an LEA from using the developed platform.

To ensure fair and comprehensive verification, the following verification criteria were developed in parallel with the development:

Table 6. Verification Criteria

Criteria	Description
Criteria Description Functionality	The App should perform all of its intended functions correctly and without errors. All features and functionalities should be thoroughly tested.
Accessibility	The App should be accessible to users with disabilities, including support for assistive technology and customizable settings to accommodate different needs.
Localisation	The App should be available in different languages and localised to meet the needs of different regions and cultures.
Usability	The App should be easy to use and navigate, with intuitive controls and a clear user interface. The app's design and layout should also be visually appealing and consistent.
Performance	The App should perform well, with fast load times and smooth transitions. The App should not freeze or crash frequently, and should be optimised for battery life and resource usage.
Security	The App should be secure and protect user data from unauthorised access or hacking attempts. The App should use encryption and secure authentication mechanisms to ensure that user data is kept confidential.

Compatibility	The App should be compatible with different devices, platforms, and screen sizes. The App should be tested on a range of devices to ensure that it works well on all of them.
Documentation	The App should have clear and thorough documentation, including user manuals and technical documentation for developers.
Maintenance	The App should be easy to maintain and update, with modular code that is easy to modify and fix. The App should also be tested regularly to ensure that it continues to perform well and meet user needs.

6.2. Results of Objective (Technical) Verification

As mentioned above, technical (objective) verification of the developed PROCTIVE web platform was conducted during the field exercises and included comprehensive measurements of all the key system parameters. The developed web platform incorporates a dedicated dashboard for viewing these parameters in real time, as the exercise evolves. As an example, Figure 17 below illustrates verification summary from the second PROACTIVE field exercise, while Figure 18 summarises results from the third PROACTIVE field exercise.

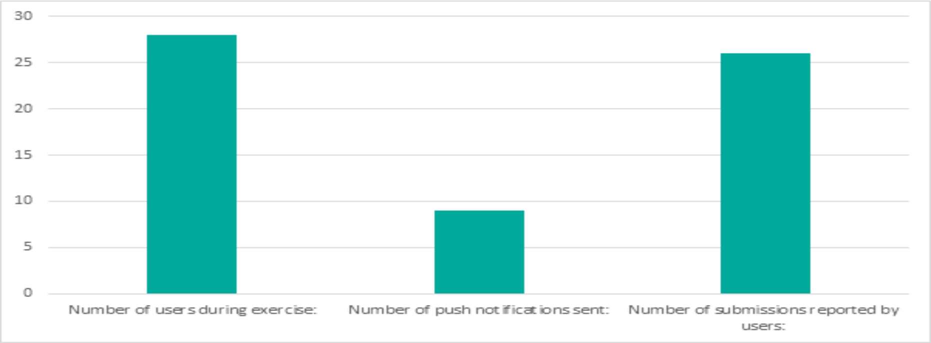
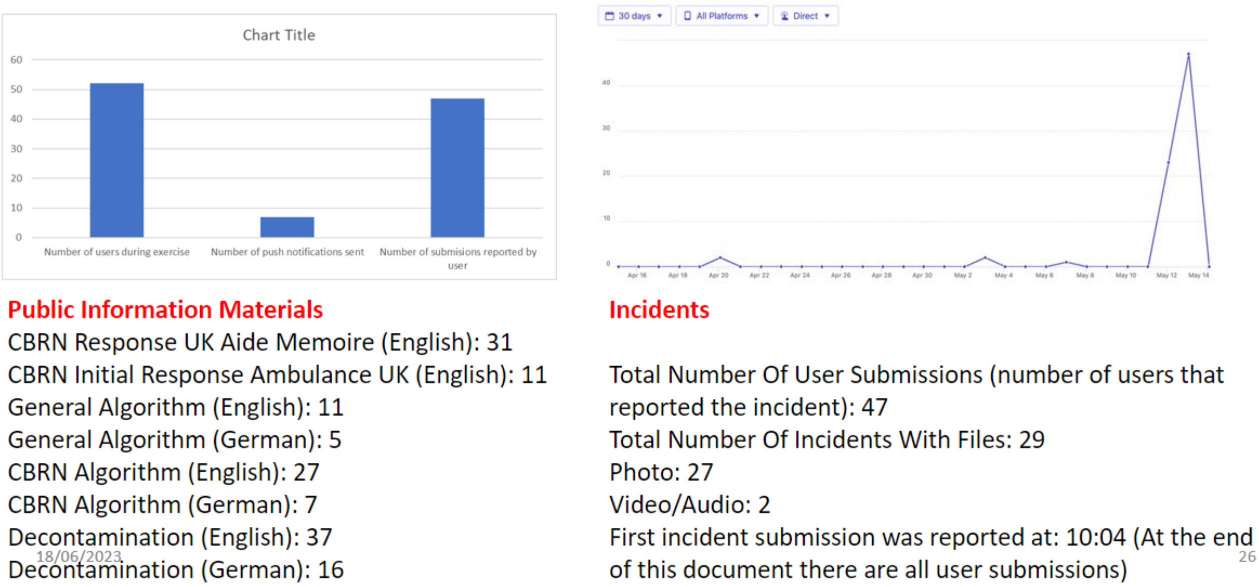


Figure 17 Summary of Objective Verification from the Second PROACTIVE Exercise



Public Information Materials
CBRN Response UK Aide Memoire (English): 31
CBRN Initial Response Ambulance UK (English): 11
General Algorithm (English): 11
General Algorithm (German): 5
CBRN Algorithm (English): 27
CBRN Algorithm (German): 7
Decontamination (English): 37
Decontamination (German): 16

Incidents

Total Number Of User Submissions (number of users that reported the incident): 47
Total Number Of Incidents With Files: 29
Photo: 27
Video/Audio: 2
First incident submission was reported at: 10:04 (At the end of this document there are all user submissions)

18/06/2023

26

Figure 18 Technical Verification Summary from the Third PROACTIVE Exercise

As it follows from these figures, the developed web Platform performed as expected with no technical issues reported during the exercise.

6.3. Subjective Verification

As part of each field training exercise, external Observers were tasked with taking on the role of a witness to the incident who would use the PROACTIVE Mobile App to a) look for information about the ongoing incident and b) report the incident. This is in line with the intended citizen end-user, as research shows that mobile apps are not likely to be used by the victims of a disaster but rather by witnesses.

The Observer Guide questionnaire included a section with roughly 20 questions focused on the app, composed of closed and open questions. The answers to the closed questions were provided on Likert-type scales and were accompanied by open questions which gave the observers the possibility to explain their answers and to give examples. Slight adjustments to the Observer Guide were made over the course of the project, to enhance clarity for example, while ensuring that the questions were similar enough to ensure cross comparison at the end. The full analysis of the Observer Guides is given in the corresponding deliverables (D6.3 [8], D6.4 [9], D6.5 [10]).

Over the course of the three field training exercises, the PROACTIVE mobile App increased in overall usability and overall usefulness (Table 7). Along those lines, so did the amount of stars the App received. This helps demonstrate the effectiveness of the iterative, co-creation processes, whereby the written feedback provided by the Observers in the Observer Guide was integrated into the version then released/used for the following exercise. By the end of the PROACTIVE project, it can be said that users find the App easy-to-use, are confident when using the App and stat that they would use the App in a real-life incident. Observers overall also agreed that the App enhances situational awareness of the population in regards to CBRNe incidents.

Table 7. Useability, Usefulness and Rating of the Mobile App

Quality/Exercise	Dortmund	Rieti	Ranst
Useable	3.99	4.58	5.04
Useful	3.90	4.64	5.01
Rating out of 5 stars, where 5 stars are the best	2.57	3.53	4.17

Specific to the web collaborative platform that we are reporting on in this deliverable (D4.2), during the 3rd field exercise a LEA consortium partner took on the role of web platform user admin, as opposed to the previous two exercises whereby RINISOFT took on the admin role. They sat at the IT desk, were the main admin for the entire exercise, reviewed citizen reports as they came in, and were responsible for drafting the notifications that were sent out. In addition, during the exercise, LEA admin provided ad-hoc comments and recommendations for future developments, which were greatly accepted and implemented. They also filled-in a specific questionnaire which is fully reported in D6.5. The summary of the results is laid out in Table 8.

Table 8. Usability, Usefulness and Rating of the Web Collaborative Platform

Quality/Exercise	Ranst
Useable	4.86
Useful	4.87
Rating out of 5 stars, where 5 stars are the best	4

These scores therefore demonstrate that the entire PROACTIVE Crisis Communication System is useable and useful for the targeted end-users (LEAs, Policy Makers and Citizens).

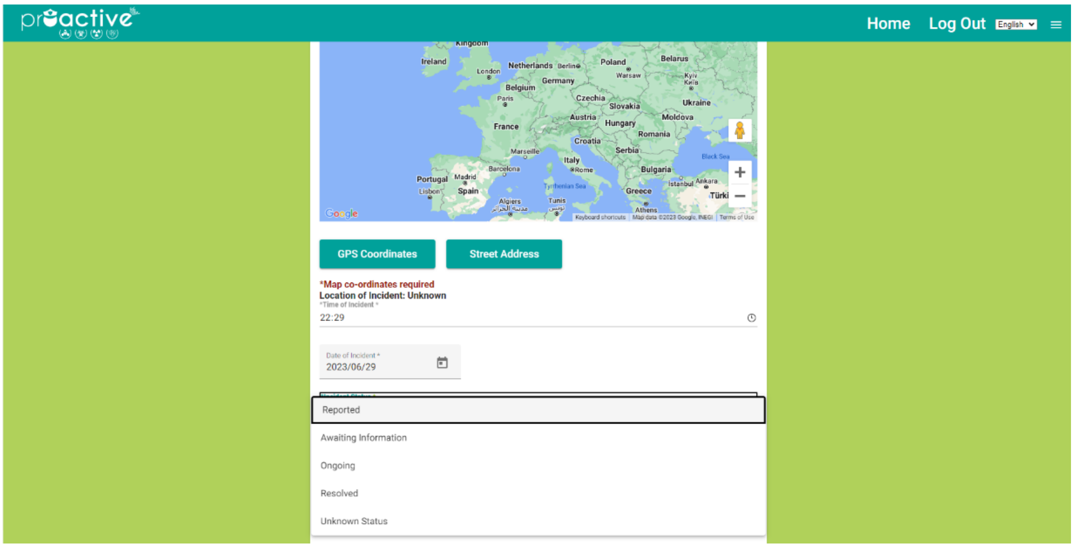
7. FUTURE WORK AND DISCUSSION

The PROACTIVE web collaborative platform has undergone long process of development, optimisations, updates and new releases and eventually performed as required during the final PROACTIVE exercise. However, the better the developed platform was performing the more recommendations and requests for modifications from the stakeholders were received, especially following the final PROACTIVE exercise and the project final conference. Most of these requests and suggestions are constructive aiming to further improve user experience. We acknowledge that this is a normal process for a digital tool which is supposed to be permanently updated and improved.

7.1. Future Work on Crisis Communications System and Collaborative Platform

Talking into account plans for commercialisation of the developed system after the completion of the project, RINISOFT has summarised all the comments and recommendations and these will be discussed with all PROACTIVE partners and communications system stakeholders. The main additional features that are considered for the implementation in the next release are as following:

- *Differentiation of the incidents on the "Incident List":* Currently all reported incidents on Incidents list are presented with the identical colours, independently of their category (currently there are 4 categories as shown in the screenshot below)



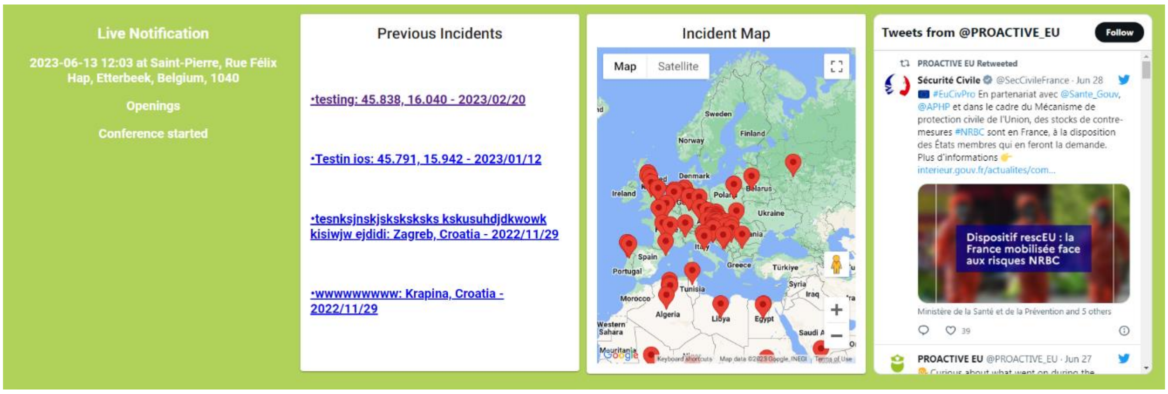
*Map co-ordinates required
Location of Incident: Unknown
*Time of Incident *
22:29

Date of Incident *
2023/06/29

Figure 19 Current Version which will be modified in future work

It was recommended to use different colours for different categories of the incidents and this recommendation will be implemented in the next release

- *Adding time stamps to "Incident List":* currently all reported incidents are permanently presented in the list of incidents as shown on the figure below:



Live Notification

2023-06-13 12:03 at Saint-Pierre, Rue Félix Hap, Etterbeek, Belgium, 1040

Openings

Conference started

Previous Incidents

•testing: 45.838, 16.040 - 2023/02/20

•Testin ios: 45.791, 15.942 - 2023/01/12

•tesnksjnskjskskskssks kskusuhdjdkwowk kisiwjw ejdidi: Zagreb, Croatia - 2022/11/29

•wwwwwwwww: Krapina, Croatia - 2022/11/29

Incident Map

Tweets from @PROACTIVE_EU

Follow

PROACTIVE EU Retweeted

Sécurité Civile @SecCivileFrance · Jun 28

#EuCivPro En partenariat avec @Sante_Gouv, @APHP et dans le cadre du Mécanisme de protection civile de l'Union, des stocks de contre-mesures #NRBC sont en France, à la disposition des États membres qui en feront la demande. Plus d'informations 👉 interieur.gouv.fr/actualites/com...

Dispositif rescEU : la France mobilisée face aux risques NRBC

Ministère de la Santé et de la Prévention and 5 others

39

PROACTIVE EU @PROACTIVE_EU · Jun 27

Curious about what went on during the

Figure 20 Another screenshot to be modified in the future work

It was suggested to modify “Incident List” by splitting it into 2 options: “Past Incidents” and “Ongoing Incidents”. From the software development perspective this makes sense and is relatively simple to implement, however, may complicate the use of the platform. Therefore, we will follow the established procedure and engage with the PROACTIVE CBRNe crisis communications system stakeholders asking for their views.

- *Adding geographical boundaries to the reported incidents:* currently reporting incidents required adding GPS coordinates of the reporter. It was suggested that a LEA who creates incident list on collaborative web platform should have an option to indicate geographical boundaries of the incident. This could be a house, street, city or country. In any case, such an option will be added in the next release, combined with advice to avoid incident area, enhancing safety of the general public.

- *Adaptation of the developed communications system for reporting technical issues on railway tracks:* currently inspection of railway tracks in done according to a schedule by dedicated personnel. Enabling public to report any potential issues will improve safety and efficiency of railway infrastructure.

- *Adaptation of the developed communications system for SMART CITY applications:* it was suggested that the developed system could be well accepted (after simple modifications) for citizen engagement in SMART CITY operations (reporting issues with roads, public transport, traffic, mass events, etc).

- *Create various groups of users:* it was suggested that from an operational point of view it will be beneficial to have different user groups, for example: LEA officers, medical personnel, vulnerable users, etc. This could be created during the registration process. While this suggestion makes sense, special consultations will be conducted with PROACTIVE partners responsible for ethical issues, ensuring that if this feature is implemented, it is implemented in full compliance with ethical recommendations.

- *Implementing bi-directional communications within the developed system*: current release support return broadcast channel, allowing collaborative platform to send simultaneous messages to all users of the toolkit. However, if different user groups are created, having individual bi-directional communications could help in improving response to the incidents (for example special messages could be sent off-duty LEA officers or medical personnel who are in the area of the incident).

- *Implement the developed toolkit with existing legacy systems*: the PROACTIVE crisis communication system is not the first and only communications system developed. There are a number of existing tools on the market, such as National warning systems, other app, proprietary tools, etc. – although none of them is CBRNe specific. It will be mutually beneficial for both the PROACTIVE and existing legacy toolkits to enable compliance and integration, eventually contributing to the overall safety during the CBRNe. More details about possible integration are outlined in the next Section.

The above listed suggestions and recommendations for future work are made by the current and potential stakeholders of the developed toolkit and as such, they will be taken very seriously. Some of these recommendations are easy to implement technically but may require additional consultations from ethics points of view. Other recommendations (like integration with existing legacy national warning systems) require close cooperation with the owners of these systems and may have admin and organisation challenges. In implementing these recommendations RINISOFT will follow the established procedure of iterative developed process developed during the project and described earlier. This will ensure that well known danger ***"better is enemy of good"*** will be avoided and future releases will be well accepted by PROACTIVE CBRNe stakeholders.

7.2. Integration with Legacy Systems

Integrating a Communications System (in our case PROACTIVE CBRNe collaborative platform and mobile app) with national information systems can be a complex process that requires careful planning, collaboration, and adherence to data security and privacy regulations. It requires collaboration between relevant stakeholders, including government agencies, platform developers, data protection officers, and legal experts.

The specific steps and considerations may vary depending on the country and the nature of the information systems involved. As an integral part of its activities in PROACTIVE Project, RINISOFT investigated this topic and identified the following guidelines which will be essential to facilitate integration of PROACTIVE CBRNe collaborative platform with national information systems [11,12]:

- ***Identify Objectives and Data Requirements***: Clearly define the objectives of integrating the platform with national information systems. Determine the specific data that needs to be exchanged between the platform and the national systems. This may include demographic information, health records, social services data, or other relevant data. Therefore, don't limit your efforts only to technical development and consider ethics and GDPR.
- ***Comply with Regulations and Standards:*** Ensure that the platform complies with all relevant national and international data protection and privacy regulations. This includes obtaining necessary permissions and consent from users and implementing robust security measures to safeguard sensitive data.

- ***Establish Data Sharing Protocols:*** Collaborate with the responsible authorities and information system owners to establish data sharing protocols. Determine the data exchange format, API specifications, and authentication methods to be used.
- ***API Integration:*** Create APIs that allow the collaborative platform to communicate with the national information systems securely. APIs provide a standardised way for different systems to exchange data.
- ***User Authentication and Authorisation:*** Implement secure user authentication and authorisation mechanisms to ensure that only authorised individuals can access sensitive information.
- ***Data Encryption***: Use encryption protocols to protect data during transmission and storage. This prevents unauthorised access to sensitive information even if intercepted.
- ***Testing and Validation:*** Thoroughly test the integration to ensure data accuracy, reliability, and consistency. Validate the data exchanged between the PROACTIVE CBRNe collaborative platform and the national systems to identify and rectify any issues.
- ***Scalability and Performance:*** Consider the potential increase in PROACTIVE CBRNe collaborative platform usage and data flow when integrated with national systems. Ensure that the infrastructure can handle increased traffic and maintain optimal performance.
- ***User Education and Training:*** Provide clear instructions and educational resources to help them understand the process.
- ***Monitoring and Maintenance:*** Continuously monitor the platform's integration with national systems to identify and resolve any technical issues promptly. Stay up-to-date with changes in national information system APIs or policies that may affect the integration.
- ***Data Anonymisation and Aggregation:*** Ensure that individual identities are protected through anonymisation techniques.
- ***Secure Data Deletion:*** Implement a mechanism to securely delete user data from the collaborative platform and the national systems if users choose to opt-out or if their data is no longer needed.

A key component in planning such an integration includes also planning verification of the developed solution, to ensure that the integration is secure, compliant with regulations, and functions as intended. RINISOFT used best practices developed during PROACTIVE project and suggested the following steps for future integration:

- ***Security Audit:*** Conduct a comprehensive security audit of both the PROACTIVE CBRNe collaborative platform and the national information systems. This audit should identify potential vulnerabilities and assess the overall security posture of the systems involved. Since PROACTIVE collaborative platform already been evaluated for “Secure by Design”, this should make the process of security audit slightly easier.
- ***Data Privacy Assessment:*** Perform a thorough data privacy assessment to identify the types of data that will be exchanged between the collaborative platform and national systems. Ensure that the collaborative platform complies with relevant data protection regulations and that user consent is obtained where necessary. Since PROACTIVE CBRNe collaborative platform already was evaluated by ETICAS for compliance with data protection regulations, this should make this step slightly easier.

- ***API Testing:*** Verify the functionality and security of the APIs that facilitate data exchange between the PROACTIVE CBRNe collaborative platform and national systems. Test various scenarios to ensure data is transmitted accurately and securely.
- ***Authentication and Authorisation Testing:*** Test the authentication and authorisation mechanisms to ensure that only authorised users can access the collaborative platform and the relevant data within the national systems.
- ***Data Accuracy and Integrity Testing:*** Verify the accuracy and integrity of data exchanged between the PROACTIVE CBRNe collaborative platform and national systems. Data should be consistent and error-free to ensure proper functioning of the platform's features.
- ***Performance Testing:*** Test the performance of the collaborative platform and the integration under various load conditions to ensure that it can handle the expected user traffic without significant issues.
- ***Compliance Verification:*** Ensure that the integration adheres to all relevant regulations and standards, such as data protection laws and industry-specific requirements.
- ***User Acceptance Testing (UAT):*** Conduct UAT with real users or representatives from the target user group to gather feedback on the platform's usability, accessibility, and overall functionality.
- ***Monitoring and Logging:*** Implement robust monitoring and logging mechanisms to track data exchanges, detect anomalies, and troubleshoot any issues that may arise after deployment.
- ***Disaster Recovery and Redundancy Testing:*** Verify that the integration includes adequate disaster recovery measures and redundancy protocols to minimise the risk of data loss or service interruptions.
- ***Legal Review:*** Seek legal review to ensure that the integration complies with all relevant laws, contracts, and agreements related to data sharing and use.
- ***Documentation:*** Throughout the verification process, document each step thoroughly and address any issues that arise promptly. Collaboration between the platform development team, national system owners, data protection officers, security experts, and legal advisors is crucial to ensure a successful and compliant integration.

The verification process described above typically involves multiple stakeholders with different areas of expertise. These stakeholders are listed in the table below.

Table 9. Stakeholders of Verification Process

Stakeholder	Role in Verification
Development Team	The development team is responsible for ensuring that the collaborative platform App meets the technical requirements for integration. They should conduct security testing, API testing, and data accuracy checks on the app's side of the integration.
Government Authorities and System Owners	The government authorities or agencies responsible for the national information systems are essential stakeholders in the verification process. They oversee the data being shared and must verify that the integration aligns with their system's security and privacy standards.

Data Protection Officers	DPOs play a critical role in assessing and ensuring data privacy compliance. They can review the platform's data privacy policies, consent mechanisms, and data handling practices to verify that user data is appropriately protected.
Security Experts	Independent security experts or security teams within relevant organisations can conduct security audits and penetration testing to identify vulnerabilities and weaknesses in the developed PROACTIVE CBRNe collaborative platform and the integration process.
User Representatives	Representatives from the target user group during user acceptance testing
Legal Advisors	Legal advisors help ensure that the integration complies with all relevant laws, regulations, contracts, and agreements related to data sharing and use.
Quality Assurance Team	A dedicated QA team can conduct comprehensive testing, including functional testing, performance testing, and regression testing, to ensure the PROACTIVE CBRNe collaborative platform functions as expected after the integration
Infrastructure and IT Teams	The IT teams managing the national information systems should verify that the platform's integration aligns with their system's architecture and requirements.

As shown in this section, integration of the PROACTIVE CBRNe collaborative platform is desirable but complex task. It requires multi-dimensional scope of activities of which technical development is important but only one of the components. In addition to steps outlined above, one more activity needs to be considered – promotion of the integrated solution to the general public. This requires a well-thought-out marketing and communication strategy which need to be developed jointly with all the stakeholders. The success of integrated PROACTIVE CBRNe collaborative web Platform relies on understanding the needs of the target audience and effectively communicating how the Platform addresses those needs. Tailoring the promotion strategy to the specific characteristics and preferences of the citizens will increase the likelihood of PROACTIVE CBRNe collaborative web Platform adoption and usage.

8. CONCLUSIONS

This document outlines the major work completed while developing the PROACTIVE Web Collaborative Platform. This platform was developed as an integral part of the overall PROACTIVE Crisis Communication System and allows exchange of best practice among LEAs providing valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRNe activities and help consolidate the EU Action Plan to enhance preparedness for CBRNe threats.

The design and development process utilised the best practice approach, ensuring that the final product meets all the requirements requested by the stakeholders. Special emphases were placed on ensuring that the developed web platform meet the need of vulnerable citizens and in “Secure by Design”.

A key complement on the overall design and development process was verification process, which included objective (technical) and subjective (questionnaire-based) verifications. The technical (objective) verification showed compliance with the developed requirements while subjective (questionnaire-based) verification shown positive acceptance by the stakeholders.

Constructive recommendations from these verifications will be implemented in the next release of the PROACTIVE web collaborative platform as an integral part of the PROACTIVE Crisis Communication System and the project’s commercial exploitation.

9. REFERENCES

1. PROACTIVE D4.1 – Report on the High-level Architecture design including an interface control document (2021). https://proactive-h2020.eu/wp-content/uploads/2021/04/PROACTIVE_20210312_D4.1_V6_RINI_Report-on-the-high-level-architecture-design_revised.pdf

2. Havârneanu, G.M., Petersen, L., & McCrone, N. (2022). Stakeholder Engagement Model to facilitate the uptake by end users of Crisis Communication Systems. In: G. Markarian, R. Karlovic, H. Nitsch, & K. Chandramouli (Eds). *Security Technologies and Social Implications.* IEEE Press. Wiley. https://doi.org/10.1002/9781119834175.ch8

3. Clegg, Dai; Barker, Richard (1994). *Case Method Fast-Track: A RAD Approach*. Addison-Wesley.

4. Petersen, L., Havârneanu, G., McCrone, N., Markarian, G. (2023). Practitioner Perspectives of the PROACTIVE CBRNe Disaster App. In: Radianti, J., Dokas, I., Lalone, N. & Deepak, K. (Eds) ISCRAM 2023 Conference Proceedings – 20th International ISCRAM Conference. pp 13-19 http://idl.iscram.org/files/petersen/2023/2502_Petersen_etal2023.pdf

5. Petersen, L., Havârneanu, G.M., McCrone, N., Markarian, Burlin, A., & Johansson, P. (2022). CBRNe, a universally designed app for that? In Grace, R., Baharmand, H. (Eds). ISCRAM 2022 Conference Proceedings – 19th International Conference on Information Systems for Crisis Response and Management, p. 836-846, ISSN 2411-3387. http://idl.iscram.org/files/laurapetersen/2022/2459_LauraPetersen_etal2022.pdf

6. PROACTIVE D8.2 – Legal and acceptability recommendations for PROACTIVE toolkit (2021). https://proactive-h2020.eu/wp-content/uploads/2021/04/PROACTIVE_20210315_D8.2_V5_ETICAS_Legal-and-acceptability-recommendations_revised.pdf

7. PROACTIVE D5.2 – Final Pre-Incident Public Information Materials for CBRNe terrorism (2023). https://proactive-h2020.eu/wp-content/uploads/2023/04/PROACTIVE_20230228_D5.2_V4_UKHSA_Final-Pre-Incident-Public-Information-Materials.pdf

8. PROACTIVE D6.3 Report on the first field exercise and evaluation workshop (2022). https://proactive-h2020.eu/wp-content/uploads/2022/07/PROACTIVE_20220630_D6.3_V4_DHPol_Dortmund-Field-Exercise.pdf

9. PROACTIVE D6.4 Report on the second field exercise and evaluation workshop (2023). https://proactive-h2020.eu/wp-content/uploads/2023/02/PROACTIVE_20230131_D6.4_V5_CBRNE_Rieti-Field-Exercise.pdf

10. PROACTIVE D6.5 Report on the third field exercise and evaluation workshop (2023). https://proactive-h2020.eu/wp-content/uploads/2023/08/PROACTIVE_20230731_D6.5_V5_UMU_Ranst-Field-Exercise.pdf

11. FEMA (2023). Integrated Public Alert & Warning System. https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system (accessed July 2023)

12. CRTC (2014). http://www.crtc.gc.ca/eng/archive/2014/2014-444.htm (accessed July 2023)

10. ANNEX 1A – CORE REQUIREMENTS

Core Requirements	
Graphic User Interface	Simple design reflecting PROACTIVE branding. Accessibility across web collaborative platform and both Mobile Applications
Direct Messaging	The ability for LEAs and Security Policy makers to interact privately. The ability for citizens to send direct messages will vary between scenarios
Forums	Open discussions between all stakeholders
Registration	Not mandatory – registering will increase level of access rights
Legal & Ethical Requirements	Working with ETICAS and CBRNE, GDPR, disclaimers and consent forms will be factored into the system
Notification of Incidents	Notify LEAs of an incident using a map-based system
Data Storage	Secure storage of information input to system
Geo-Location	The ability for the system to recognise the location of an incident(s)
Information Sharing	Ability to share pre-incident information with all users in multiple formats (text, video, audio)
Missing Loved Ones	Ability to locate humans and pets during an incident
Contact Information	List of organisations relevant to vulnerable groups

11. ANNEX 1B – FUNCTIONAL REQUIREMENTS

Functionality Requirements for Field Exercises	
Inter-Agency Information Sharing	The ability to converse directly with relevant stakeholders to discuss operational aspects in terms of information sharing
Pre-Incident Information	Information from T5.1 will be available in the system for users to reference
Post Incident Information	Information post incident to be provided to stakeholders, specific to the scenario exercise as a lesson learnt.
Links to Available National Apps	Countries with existing Apps for crises events will have the link signposted in the PROACTIVE Platform
Notification Alerts	Live notifications to be provided by LEAs at all stages of the incident
Existing News Feeds	News feeds from the relevant countries/ areas will be linked to the PROACTIVE Mobile Application, to create a central hub for information
Data Analysis	LEAs will have access to data, specifically number of users on the platform and at what stages the platform was used etc.