D4.16
Communications to Remote Areas – Design and Specifications – Draft

Instrument	Collaborative Project
Call / Topic	H2020-SEC-2016-2017/H2020-SEC-2016-2017-1
Project Title	Multi-Hazard Cooperative Management Tool for Data Exchange, Response Planning and Scenario Building
Project Number	740689
Project Acronym	HEIMDALL
Project Start Date	01/05/2017
Project Duration	42 months
Contributing WP	WP 4
Dissemination Level	PU
Contractual Delivery Date	M22
Actual Delivery Date	02/04/2019
Editor	Diana Mathew (AVA)
Contributors	Diana Mathew, Joseph Muna (AVA), Benjamin Barth (DLR)

Document History			
Version	Date	Modifications	Source
0.1	20/04/2018	ToC and first draft	AVA
0.11	15/12/2018	Updates after EUW2 in Glasgow	AVA DLR
0.47	25/03/2019	Draft for QA to CTTC	AVA DLR
1.0.D	02/04/2019	Final version submitted to DLR for approval	AVA
1.0.F	02/04/2019	Final version submitted to the portal	DLR

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACAP	Alerting Channels Access Points
AG	Alerting Gateway
AOI	Area of Interest
AVA	Avanti Communications LTD
CAP	Common Alerting Protocol
CTTC	Centre Tecnològic de Telecomunicacions de Catalunya (Catalan Tecnological Telecommunications Centre)
C&C	Command & Control
DLR	Deutsches Zentrum für Luft- und Raumfahrt e.V. (German Aerospace Center)
EC	European Commission
EUW	End Users Workshop
FCP	Forward Command Post
FR	First Responder
GUI	Graphical User Interface
IG	Information Gateway
IPR	Intellectual Property Right
IV&V	Integration , Verification & Validation
JSON	JavaScript Object Notation
LU	Local Unit
MCE	Message Composition Engine
SatCom	Satellite Communication
SP	Service Platform
SR	System Requirement
TR	Technical Requirement
UDP	User Datagram Protocol
UR	User Requirement
URL	Uniform Resource Locator
VSAT	Very Small Aperture Terminal
Wi-Fi	Wireless Fidelity

Intentionally blank

Executive Summary

This deliverable document presents the work carried out as part of Task 4.5 (Communication to Remote Areas) in the first two release phases, Releases A and B, of the HEIMDALL project. The main objective of this document is to provide details about the design requirements and specifications of the Information Gateway (IG) and SatCom modules of the HEIMDALL system, which together make the 'communication to remote area' functionality possible. This deliverable thus includes the technical requirements derived from the user and system requirements identified in D2.6 [4] and D2.7 [5], scope and functionalities offered by the modules under consideration and the test results of the implemented features. This is an initial version and will be followed by the final version, D4.17, in M38 [7].

The Information Gateway (IG) module facilitates population awareness and information sharing between the first responder (FR) users and the web-based HEIMDALL users. The IG, via the smartphone application, allows the FRs access to information available on the system and allows receiving messages from the command and control (C&C) centre. Additionally, the IG offers a multi-language capable alerting service for the public. The IG is an augmented version of the alerting gateway (AG) messaging service developed as part of the Alert4All [1] and PHAROS [2] projects. On one end, the IG is connected to the rest of the modules in the HEIMDALL network via the service platform (SP) and on the other end it connects to the HEIMDALL mobile application via internet.

As the hazard events usually take place in remote locations with no/limited internet connectivity or result in disrupting the communication infrastructure of the location, a satellite-based broadband connection is envisaged to overcome such situations. A portable, easily deployable, *Ka*-band based Very Small Aperture Terminal (VSAT) kit with Wireless Fidelity (Wi-Fi) capability will be used to provision an on-demand high-throughput satellite-based broadband connectivity for the first responder users in the field.

The Information Gateway functionalities implemented and integrated for Release-A were verified against specific test cases and also presented to the end-users for feedback at the end user workshop (EUW2) in Glasgow in October'18. Modifications and new technical requirements based on their feedback will be included in the upcoming releases (B, C) of HEIMDALL and documented in D4.17 [7].

A mobile application is being developed for HEIMDALL as part of Task 5.3 (Crowdsourced and First Responders data). As this work is closely related to the work reported here, technical requirements identified for the mobile application are included in this document in the interim to make it easier to keep track of the requirements definition of the functionalities in the initial implementation and integration stages. These requirements will be moved to a separate deliverable, D5.7 (due M38), at a later stage [6].

1 Introduction

To address the issue of providing a reliable communication link to first responders in the field in remote areas with no/limited service, HEIMDALL is proposing a satellite based broadband connection. Communication to remote areas or areas experiencing connectivity issues during an event is envisaged to be served by the Information Gateway (IG).

Work which forms part of T5.3/D5.7 (*First Responders Data Module Design)* is included as well which will be moved to a standalone deliverable at a later stage.

This document is further organised as follows:

- Section 2 describes the technical specifications captured so far for the IG module, the satellite-based broadband connection and the smartphone application, along with their interface requirements.
- Section 3 describes the context of the IG module, the Satellite Communication (SatCom) connection and the mobile-app within the overall HEIMDALL architecture
- Section 4 provides a brief description of the functionalities offered by the IG and the mobile application at the end of Release-A phase.
- Section 5 provides the IV&V test procedures and results of the IG and the application for the Release- A phase.
- Finally, Section 6 summarises and concludes the document. References are provided in Section 7.

2 Technical Requirements

This section describes the technical requirements (TRs) for the information gateway (IG) and the satellite communication (SatCom) modules of the HEIMDALL platform. The TRs have been derived from the user requirements (URs) and system requirements (SRs) identified during the end user workshops (EUWs) and progress meetings in the initial 18 months of the project. These URs and SRs have been documented in D2.6 [4] and D2.7 [5].

Technical requirements for the smartphone application for first responders are also included here in the interim to make it easier to keep track of the requirements definition of the functionalities in the initial implementation and integration stages. These requirements will be later moved to a standalone document D5.7 [6] due M38.

2.1 Information Gateway

The alerting gateway (AG) developed as part of the Alert4All [1] and PHAROS [2] projects to improve population awareness will be used to send information messages to first responders. HEIMDALL will see augmentation of the AG into a secure information gateway to grant access for first responders to the information available on the platform.

2.1.1 Interface Requirements

The Information Gateway (IG) is connected on one hand to the HEIMDALL network via the Service Platform (SP) and on the other hand to the Internet for providing the information to the first responders in the field and to model a channel to the public. Via the Internet connection the Satellite Network can be accessed for information exchange. For verification of the interface requirements, it shall be tested whether or not the specified interface features of the IG are working properly.

2.1.1.1 Hardware Interfaces

The IG should be connected to the internet and HEIMDALL network via Ethernet port.

2.1.1.2 Software Interfaces

The IG shall interface via RESTful Web services to:

- The SP to access the user and scenario management as well as the situation awareness tools;
- The receiver application;
- The Graphical User Interface (GUI) to let a user control the IG.

These requirements relate to: Sys_DSC_12, Sys_DSC_10, Sys_DSC_11, Sys_DSC_5, Sys_DSC_1, Sys_DSC_2.

2.1.1.3 Communication Interfaces

The IG shall use either HTTP or, for secured connection, HTTPS to connect to the HEIMDALL network and the internet.

These requirements relate to: Sys_DSC_26.

2.1.2 **Functional Requirements**

2.1.2.1 Short Term Features

Table 2-1: Technical Requirement TR_Com_1

Requirement ID:	TR_Com_1
Related SR(s):	• Sys_DSC_8
Description: The IG shall offer means to keep the population informed.	
Rational: In order to mitigate people at risk and casualties the population must be informed. The IG is the technical module that shall include this functionality.	
Stimulus: The user starts a process to inform the public.	
Response: Information is distributed via dedicated channels.	
Verification Criterion: Information can be distributed using the IG	
Notes: Standards should be used.	

Table 2-2: Technical Requirement TR_Com_2

Requirement ID:	TR_Com_2
Related SR(s):	• Sys_DSC_5 • Sys_DSC_8
Description: The IG shall be able to transmit alert messages to the population.	
Rational: The population shall be informed about risks, hazards and disasters. Alert messages are common and successful mean to inform the public.	
Stimulus: The user creates an alert message at the IG using the GUI and triggers the transmission of it.	
Response: IG dispatches an alert to the connected networks.	
Verification Criterion: An alert is created at the IG and dispatched. The alert is successfully received and displayed at the receiver application.	
Notes: none	

Table 2-3: Technical Requirement TR_Com_3

Requirement ID:	TR_Com_3
Related SR(s):	• Sys_DSC_5 • Sys_DSC_8
Description: The IG shall be able to create alert messages.	

Rational: In order to transmit messages to the public they need to be created.
Stimulus: The user uses to GUI to create an alert message at the IG.
Response: The IG informs the user about the status of the message under creation.
Verification Criterion: Using the GUI an alert message can be create at the IG.
Notes: Standards should be used.

Table 2-4: Technical Requirement TR_Com_14

Requirement ID:	TR_Com_14
Related SR(s):	• Sys_DSC_31
Description: The IG shall be able to consider predefined areas on different levels (municipality/region/state).	
Rational: Different user profiles look at different scales of the area. The IG must be able to cope with all area sizes.	
Stimulus: GUI sends the selected area.	
Response: The area is updated by the IG.	
Verification Criterion: The area shown in the alert message is the one selected by the user.	
Notes: None	

Table 2-5: Technical Requirement TR_Com_15

Requirement ID:	TR_Com_15
Related SR(s):	• Sys_DSC_31
Description: The IG shall be able to consider different types of areas: • Circles • Polygons • Predefined areas • Address	
Rational: Offering multiple options to set the area is very flexible and allows the user to select the best possible way for the current situation.	
Stimulus: GUI sends the selected area.	
Response: The area is updated by the IG.	
Verification Criterion: The area shown in the alert message is the one selected by the user.	
Notes: None	

Table 2-6: Technical Requirement TR_Com_16

Requirement ID:	TR_Com_16
Related SR(s):	• Sys_DSC_33
Description: The IG shall be able to consider different types of users as recipents within the private message.	
Rational: The user wants to address sub-groups within the organisation.	
Stimulus: User selects a sub-group for which the message is intended.	
Response: The message is send to the corresponding addresses of the sub-groups.	
Verification Criterion: If a sub-group is selected as recipient, the IG sends the addresses of the sub-group to the address field of the Common Alerting Protocol (CAP) message.	
Notes: Address field is used instead of sub-categories in the CAP standard.	

Table 2-7: Technical Requirement TR_Com_17

Requirement ID:	TR_Com_17
Related SR(s):	• Sys_DSC_34
Description: The IG shall shall be able to allow the selection among multiple channels.	
Rational: In order to allow the user the selection of dedicated channels the IG must consider this.	
Stimulus: User selects/deselects a channel for alerting.	
Response: The IG updates the configuration for the dissemination.	
Verification Criterion: Different channels are selected/ deselected and the IG updates the config files.	
Notes: None	

Table 2-8: Technical Requirement TR_Com_21

Requirement ID:	TR_Com_21
Related SR(s):	• Sys_DSC_42
Description: The IG shall be able to share pictures.	
Rational: Maps are provided in digital format as pictures.	
Stimulus: A picture is set as an attachment to an alert message.	
Response: The IG attaches the picture to the alert message.	
Verification Criterion: The user in the field can access the data available at the local unit (LU).	

Notes: none

2.1.2.2 Mid-Term Features

Table 2-9: Technical Requirement TR_Com_4

Requirement ID:	TR_Com_4
Related SR(s):	• Sys_DSC_15
Description: The IG shall allow users in the field to access all data or specific data sets.	
Rational: Users in the field, especially in disaster situations or rural areas, have limited access to networks. The IG shall be the mean which they can use the get the necessary information.	
Stimulus: Users in the field request information from the IG.	
Response: The IG answers with the requested information if available.	
Verification Criterion: The user can connect to the system from the field and receives the requested information.	
Notes: Standards should be used.	

Table 2-10: Technical Requirement TR_Com_5

Requirement ID:	TR_Com_5
Related SR(s):	• Sys_DSC_16
Description: The IG shall consider access rights for each user/profile.	
Rational: In order to design a secure system the IG must be able to interact with the access control methods of the system to ensure that only authorized personal can access the system via the IG.	
Stimulus: Credentials for the access to the system are transferred for login.	
Response: The system grants access upon successful login.	
Verification Criterion: User with an account and the corresponding rights can access information available for their profile. Attackers with invalid credentials cannot access the system via the IG.	
Notes: Standards should be used.	

Table 2-11: Technical Requirement TR_Com_18

Requirement ID:	TR_Com_18

Related SR(s):	• Sys_DSC_36
Description: The IG shall be able to provide information about who has access to which data.	
Rational: In order to allow the user to have a good picture of the situation it is necessary that he knows who has access to the data.	
Stimulus: User requests an overview of a data set about who has the access rights.	
Response: The IG answers with the access rights.	
Verification Criterion: The correct access rights for the data set are shown.	
Notes: none	

Table 2-12: Technical Requirement TR_Com_19

Requirement ID:	TR_Com_19
Related SR(s):	• Sys_DSC_36
Description: The IG shall be able to show the incident commander who has accessed the data already	
Rational: In this way the incident commander can have an overview if there is a lack of information at some point.	
Stimulus: The incident commander asks about the status of distribution for some information.	
Response: System returns if someone with access rights already has accessed the data.	
Verification Criterion: The incident commander can identify if a data set has been accessed by another user.	
Notes: none	

Table 2-13: Technical Requirement TR_Com_20

Requirement ID:	TR_Com_20
Related SR(s):	• Sys_DSC_36 • Sys_DSC_18
Description: The IG shall be able to share data and data sets with users in the field.	
Rational: In order to share the information with users in the field the IG is the interface.	
Stimulus: Data is requested by the user in the field.	
Response: The IG forwards the information tailored to the channel quality.	
Verification Criterion: The user in the field can access the data available at the LU.	
Notes: none	

2.1.3 **Non-functional Requirements**

Table 2-14: Technical Requirement TR_Com_11

Requirement ID:	TR_Com_11
Related SR(s):	• Sys_DSC_6
Description: The IG shall be able to connect to communication networks.	
Rational: In order to forward messages and connect first responders the IG must be able to connect to communication networks.	
Verification Criterion: The IG can establish a connection to other system components according to the overall system architecture.	
Notes: Standards should be used.	

Table 2-15: Technical Requirement TR_Com_12

Requirement ID:	TR_Com_12
Related SR(s):	• Sys_DSC_26
Description: The IG shall be connected to secure communications links.	
Rational: The links to and from the IG must be secured to ensure security of the whole system.	
Verification Criterion: An attacker outside of the secured network tries to access the IG which shall not be successful.	
Notes: Standards should be used.	

2.2 Satellite Communication

Natural disasters like wildfires, floods, landslides and so on, usually occur in remote areas and additionally often result in destroying the existing communication infrastructure of the area. These factors present difficulties such as low quality/ congested/ non-existent communication channels for emergency response operation teams. HEIMDALL proposes to overcome this situation by using satellite-based internet connectivity. The proposed solution will make use of a rapidly deployable, lightweight and portable VSAT operating in Ka-Band. In addition, a Wi-Fi access point will be set-up, allowing all authorised first responders to communicate with the Forward Command Post (FCP) and the C&C via the HEIMDALL web-platform and/or the mobile application. The satellite broadband connection will also allow real-time monitoring and communication with the drones system. The VSAT employed will be a Sematron Flyaway terminal consisting of a VSAT antenna, modem, Wi-Fi router and battery. Specifications of the VSAT kit will be detailed in the final issue of this document.

2.2.1 **Interface Requirements**

2.2.1.1 Hardware Interface

The VSAT is a standalone unit. The smartphones will connect to the portable VSAT terminal via an integrated Wi-Fi router.

2.2.1.2 Software Interface

Not applicable.

2.2.1.3 Communication Interfaces

Any standard IP data protocol such as HTTP or HTTPS can be used to connect to remote severs.

2.2.2 **Functional Requirements**

2.2.2.1 Mid-term Features

Table 2-16: Technical Requirement TR_Com_13

Requirement ID:	TR_Com_13
Related SR(s):	• Sys_DSC_6 • Sys_DSC_14 • Sys_DSC_26 • Sys_DSC_30
Description: An alternative secure communication system that is easily deployable by the user in a disaster area shall be possible. Ka-band satellite broadband connectivity shall be made possible using a rapidly deployable, lightweight and portable Ka-band VSAT.	
Rational: The location of some incidents is sometimes out of range of terrestrial communications networks and/or communication networks can be damaged in the aftermath of an event. Therefore, the system must provide an alternative way of communications.	
Stimulus: An incident takes place in an area with no connectivity via terrestrial	

communications networks.
Response: A Ka-band satellite terminal shall be deployed providing an alternative communication link to the first responders and the FCP.
Verification Criterion: A Ka-band satellite terminal is installed in the incident area. The FR/FCP is able to connect to the satellite broadband network using a mobile phone/laptop and check that they can reach the internet.
Notes: none

2.2.3 **Non-Functional Requirements**

No non-functional requirements have yet been identified as part of the requirements definition exercise.

2.3 Smartphone Application

A smartphone application based on Android operating system is being developed as part of the HEIMDALL project to allow real-time communication with the first responder users on the field. The app communicates with the HEIMDALL platform via the information gateway (IG), making use of internet connectivity available through the terrestrial communication infrastructure or the satellite-based broadband. In the first instance, the app will be made available only to the first responders.

2.3.1 **Interface Requirements**

2.3.1.1 Hardware Interface

<*To be included in D5.7*>

2.3.1.2 Software Interface

<*To be included in D5.7*>

2.3.1.3 Communication Interface

Alert messages sent via the GIS engine shall be received in the mobile application via the Common Alerting Protocol (CAP). More details will be provided in D5.7.

2.3.2 **Functional Requirements**

2.3.2.1 Short-term Features

Table 2-17: Technical Requirement TR_DataFR _1

Requirement ID:	TR_DataFR_1
Related SR(s):	• Sys_GuiApp_1 • Sys_GuiApp_2
Description: A mobile application shall be implemented for both public (long-term) and first responders (in the short-term).	
Rational: Both public and first responders require communicating with the system or receiving updates from the system.	
Stimulus: The system is about to dispatch an alert to the public and first responders that needs to be received.	
Response: A mobile application shall be implemented to receive that particular alert.	
Verification Criterion: Check the availability of a mobile application for both public and first responders.	
Notes: none	

Table 2-18: Technical Requirement TR_DataFR_2

Requirement ID:	TR_DataFR_2
Related SR(s):	• Sys_GuiApp_3

Description:
The first responders' mobile application shall be capable of logging in only first responder users.
Rational: Logging-in enables to ensure that only first responders' users will access the data and services restricted to first responders.
Stimulus: First responders' users require access to the mobile application.
Response: System obtains first responders user's credentials, double check the validity of this information against the stored data in the database and, decides whether to grant access to the mobile application or not.
Verification Criterion: Login to the mobile application as first responders' user and make sure that the mobile application grants access.
Notes: none

Table 2-19: Technical Requirement TR_DataFR_3

Requirement ID:	TR_DataFR_3
Related SR(s):	• Sys_GuiApp_4 • Sys_GuiApp_9
Description:	
The mobile application shall receive alert messages that are sent from the system.	
Rational: During an incident, the system will send alert messages to public and first responders to alert them of a risk and keep them updated.	
Stimulus: The system dispatches an alert message.	
Response: The mobile application receives the alert message and is displayed to the user.	
Verification Criterion: An alert is created at the GUI and dispatched. The alert is successfully received and displayed at the mobile application.	
Notes: none	

Table 2-20: Technical Requirement TR_DataFR_4

Requirement ID:	TR_DataFR_4
Related SR(s):	• Sys_GuiApp_5 • Sys_DataEx_7 • Sys_DataEx_8 • Sys_DataEx_9 • Sys_DataSitu_2
Description:	
The mobile application shall be capable of sending photos, extra incident details, incident reports, user's information, et al. to the HEIMDALL system. Also, the mobile application shall make sure to distinguish whether this information is sent from the public or from a first responder's user by including user's metadata.	

Rational: Relevant information received from both public and first responders might be extremely value for situational assessment, incident awareness, decision support, et al.
Stimulus: A user requires sending some relevant information to the system regarding an ongoing incident.
Response: The system is able to receive this information and display it in the GUI.
Verification Criterion: Some relevant information is sent from the mobile application to the system. Once received this information, the GUI will display it to the user.
Notes: none

Table 2-21: Technical Requirement TR_DataFR _5

Requirement ID:	TR_DataFR_5
Related SR(s):	• Sys_GuiApp_6 • Sys_GuiApp_7 • Sys_DataEx_1
Description: The mobile application shall be capable to track and display the location of all first responders during an incident.	
Rational: First responders need to be aware of the location of all first responders during an incident at all times.	
Stimulus: The mobile application tracks the location of the first responders and sends updates to the system.	
Response: The mobile application is able to display the latest location of other first responders on a map.	
Verification Criterion: The mobile application shall track and display the latest location of other first responders on a map.	
Notes: none	

Table 2-22: Technical Requirement TR_DataFR _6

Requirement ID:	TR_DataFR_6
Related SR(s):	• Sys_GuiApp_8 • Sys_DSC_23
Description: The mobile application shall provide a chat feature to first responders and FCP users to easily communicate with the HEIMDALL platform.	
Rational: FR/ FCP users usually need to communicate with other users on the field and the command centre.	
Stimulus: A FR/ FCP user sends a chat message to a user (1) at the command and control centre and (2) on the field.	
Response: The HEIMDALL platform (case 1)/ mobile application (case 2) is able to receive	

the chat message.
Verification Criterion: A message is sent from a FR/ FCP user to another FR/ FCP user and also to the C&C. The mobile application/ web- GUI shall be able to receive this chat message at the other end.
Notes: none

2.3.2.2 Mid-term Features

Table 2-23: Technical Requirement TR_DataFR_7

Requirement ID:	TR_DataFR_7
Related SR(s):	• Sys_GuiApp_10
Description: The mobile application shall allow the users to save a map of the Area of Interest (AOI) in the cache memory of the user's smartphone.	
Rational: The user would need to be able to have directions to the AOI even if the connectivity to the internet is absent/ limited.	
Stimulus: User locates the AOI on the map and saves a local copy for offline use.	
Response: A copy of the directions is saved locally on the user's smartphone.	
Verification Criterion: The user can retrieve the copy of the map saved on his/her smartphone.	
Notes: none	

Table 2-24: Technical Requirement TR_DataFR_8

Requirement ID:	TR_DataFR_8
Related SR(s):	• Sys_GuiApp_11
Description: The mobile application shall allow the users to send and receive waypoints.	
Rational: This will allow the first responder users to send and receive any updates to the default/pre-determined route based on any changes happened during an incident.	
Stimulus: The pre-determined route to a location has been modified	
Response: 1) The C&C user creates the new route on the GUI and sends it to the FR user 2) The FR user plots the new route and shares it with the C&C centre	
Verification Criterion: • A registered first responder user is able to create and send waypoints to the C&C centre. • The first responder user is able to receive and view the waypoints received from the C&C centre on the app.	

Notes: none

2.3.3 **Non-Functional Requirements**

No non-functional requirements have yet been identified as part of the requirements definition exercise.

3 Reference Architecture

3.1 Overall HEIMDALL architecture

Figure 3-1 shows the overall architecture of the HEIMDALL system. The Intelligent Gateway (IG) module, SatCom module and the Receiver App are highlighted in red boxes.

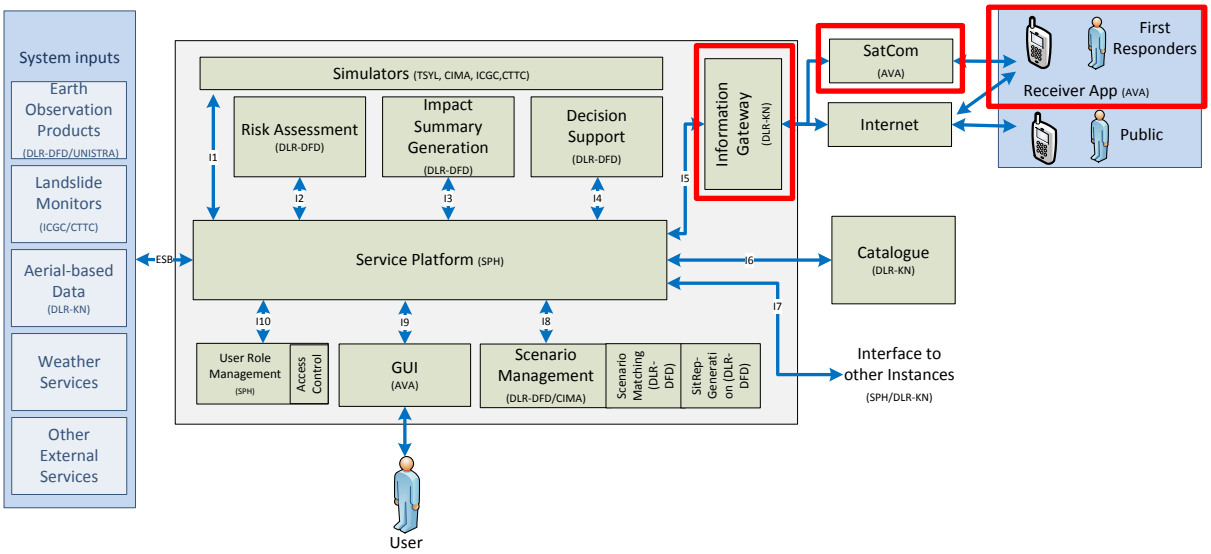

Figure 3-1: HEIMDALL Architecture

3.2 Information Gateway

As depicted in **Figure 3-1**, the central element between the HEIMDALL system and the first responders (FR) in the field and the public is the information gateway (IG). On HEIMDALL platform, it is connected via the service platform (SP) to the scenario management, situation assessment modules and the GUI for information provision to the users in the field offering a FR information services as summarized in **Table 3-1**. The FR can use the HEIMDALL smartphone application to access the information available on the system and can receive messages from the command and control (C&C) centre.

Another service offered by the IG is an alerting service for public awareness. Alert messages are composed by the user using the web-based GUI and can be forwarded to the smartphone application that can also be used as alerts receiver. The alerting service is based on the approaches of the PHAROS and Alert4All projects and offers multi-language capabilities and easy message composition features and enables the possibility to use a variety of communication channels as shown during these projects. For HEIMDALL we focus on terrestrial internet access and satellite-based broadband, only.

Table 3-1: Information gateway inputs/outputs

Products and/or Services	**Inputs needed**	**Provided by**	**Used by**
FR information service	Situation Report (SitRep) Scenario User Role Management (UeRM)	Situation Assessment Scenario Management	Smartphone application

Alerting service	CAP message	GUI	Smartphone application

Table 3-2: Interface to the Service Platform (SP)

Interface	Short description	Methods	Protocol
I5	RESTful web service interface	GET, POST, PUT, DELETE	HTTP(S)

3.3 Satellite Communication

As shown in the overall architecture diagram, the satellite communication module forms a data link between the core HEIMDALL platform and the HEIMDALL mobile application, facilitating data transfer in the form of voice, video and messaging. The SatCom module is a standalone entity with no hardware interface to any of the other HEIMDALL modules.

Table 3-3: Communication to Remote areas inputs/outputs

Products and/or Services	Inputs needed	Provided by	Used by
Ka-band satellite communications	Successful configuration and installation	N/A	First Responders

4 Module Functionality

This section shall describe the different building blocks within the IG and SatCom modules.

4.1 Information Gateway

The Information Gateway (IG) design has been based on the Alerting Gateway (AG) which has been developed in the framework of the EU FP7 projects Alert4All [1] and PHAROS [2] and therein represented the communication hub responsible for dispatching alert messages composed by the operator via the web-based GUI. It is further extended in HEIMDALL in order to process and forward situation awareness information and scenarios for FRs in the field.

Components of the IG are shown in Figure 4-1. The FR information service is included in the web server of the alerting service with the difference that it uses the same server for forwarding the information as well. It has access to the local database and configuration files. The alerting service makes use of some more components, inherited from previous designs and explained in detail in the following. This includes the functions that implement the interface with the SP, the AG main processor; the message composition engine (MCE), the interface with the alerting channels access points (ACAPs), the local database and the configuration files.

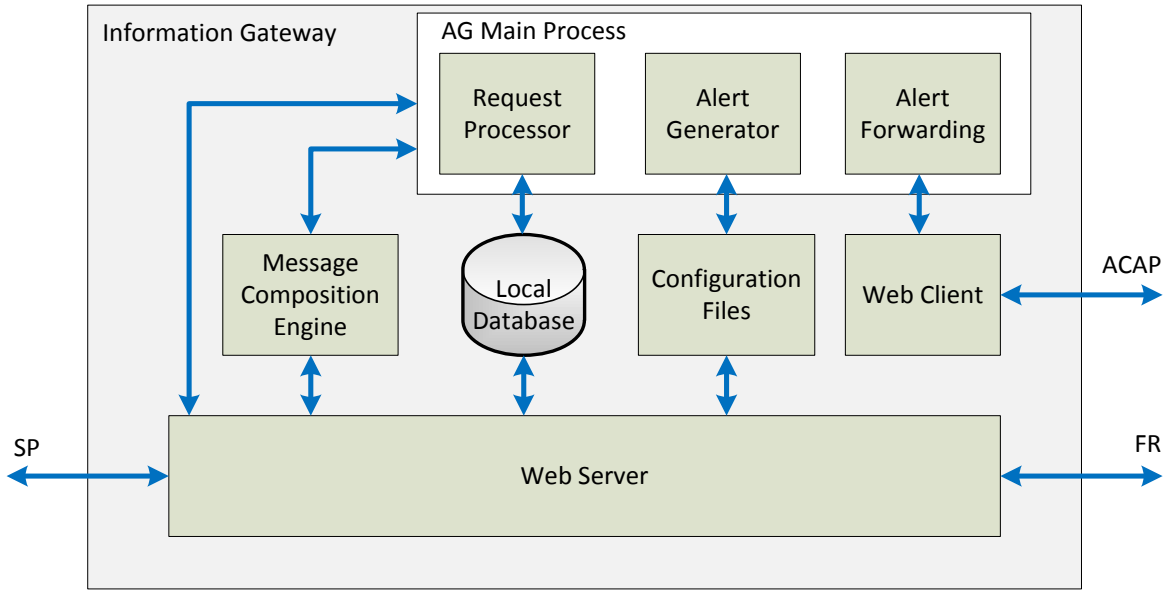

Figure 4-1: Information Gateway (IG) components

The interface between the IG and the SP is based on web services and, hence, it consists of web server, able to receive and process the corresponding web requests. The web server implements the following functions for the alerting service:

- Receive and process the web requests from the SP and send responses;
- Generate common alerting protocol (CAP) [3] files out of the SP inputs for internal use;
- Trigger the MCE;
- Update the local database with the requests for documentation purposes;
- Trigger the process in the ‘AG Main Process’ module that correspond to the received requests;

The web server provides the web services in a PHP script described in more detail in section 5.1. As already mentioned, the functionality of the web server for the FR information service is extended since it will also receive requests to and from FRs as well as process situation awareness and scenario information.

In order to create a human readable version of the alert message to be distributed, the MCE is called by the web server functions which has been developed and enhanced in PHAROS and Alert4All. The MCE is provided as a Java executable. The IG uses the MCE to set the text in the description, the instruction and the headline fields of the CAP, using the information in the other CAP fields to formulate a human-readable version of the alert message.

The *AG main process* module in the IG is structured in three main parts:

- The request processor is the module which communicates with the web server in the SP interface and triggers the corresponding internal processes that can either be the alert generator or the alert forwarding;
- The alert generator takes care of generating the alert message in the appropriate format to be transmitted and decoded;
- Finally, the alert forwarding module takes care of intelligent forwarding of alert messages (and report requests) towards the ACAPs.

The *AG main process* and the interface to the ACAPs are combined in a multi-thread C++ program. The main process is triggered by the web server at the SP interface. If a dispatch command is initiated by the user at the GUI, the web server sends the corresponding CAP file and the list of the selected channels via User Datagram Protocol (UDP) socket to the main process. It is received by the request processor, which parses the CAP file and sets the channels accordingly at the alert forwarding entity. The alert generator converts the parsed CAP to different formats. It is possible to convert it to the A4A-protocol and JavaScript Object Notation (JSON) (see section 5.1).

4.2 Satellite Communication

The satellite-based broadband connectivity for the users on the field will be provided using a light weight, robust, quick-deployable Sematron Flyaway terminal. A high level schematic of the end-end connection facilitated by the satellite terminal is shown in Figure 4-2.

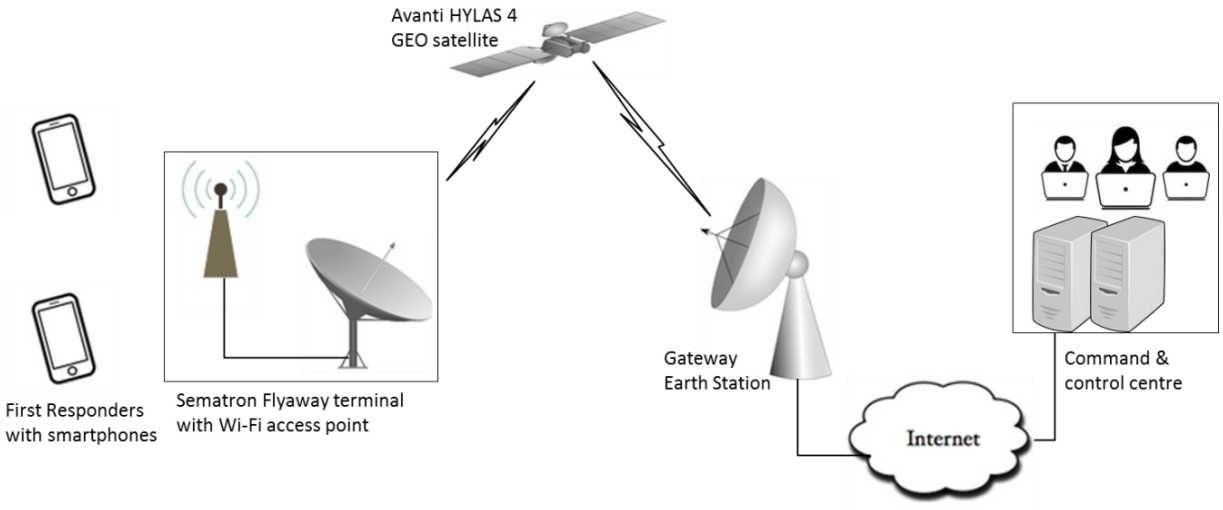

Figure 4-2**:** Schematic architecture diagram of the end-end communication link in HEIMDALL with rapid deploy satellite communication

The VSAT terminal design includes a 1m high gain carbon fibre reflector, ‘no-tools’ assembly, folding feed arm assembly, quick deploy tri-pod, inclinometer and fine adjust on Azimuth and Elevation. The tri-pod has detachable feet to allow for ground anchors to be fitted, ensuring maximum stability for reliable operation. A Wi-Fi modem and router can be plugged to the VSAT unit to set-up a Wi-Fi access point. Satellite broadband connectivity is provided by Avanti over its HYLAS 4 geo-stationary satellite covering Europe.

5 Technical Specification

5.1 Information Gateway

As already introduced in the previous section, the IG provides two services, the alerting service and the FR information service.

For the alerting service, alert messages are created through the user interface. The internal format to create and store locally the alert messages is the Common Alerting Protocol (CAP) [3]. Users will create the message using the different menus provided in the UI (using pre-defined alerting libraries) or manually introducing text in the given text boxes. The provided data items will be gathered at the IG and used to populate a CAP file containing the relevant alert information. Once all the mandatory data items have been inserted by the user, the possibility to disseminate the alert message will be available at the UI.

When receiving the request to disseminate the message, the IG triggers the internal creation of the message according to the selected alerting channels. The mapping between the alerting channels and the format used for each of them is stored in the dedicated configuration files, for the pre-operational version. In a general case, the following formats are provided by the alert generator module:

- **Common Alerting Protocol (CAP)** is an XML-based message format which is used by a wide number of alerting systems, thus allowing interoperability between already existing systems. By providing CAP compatibility, the system is able to input alerts in already operating systems based on the CAP format.

- **A4A Protocol**: The Alert4All protocol was designed and first implemented within the Alert4All project [1] in order to overcome the limitations that the transmission of CAP messages presented in narrowband channels. The A4A protocol is based on the use of extensible headers which include the encoded version of the message as well as the verbose version, if needed. The principle used for encoding the alert message information is based on the use of alerting libraries. These alerting libraries provide, for each information item to be included in the alert message according to the CAP protocol, a series of options to build the message. According to the chosen options, an encoded version of the alert message will be created and disseminated.

The alert forwarding then dispatches the alerts in the proper format to the alerting channels. Therefore, its Uniform Resource Locator (URL) encodes information of the message for the ACAPs. The URL used by the alert forwarding module has the following structure:

```
http://{user}:{password}@{ACAP-IP}/{path}/{reqType}/{IG-ID}/{incidentId:messagId}
```

If no authentication is required, the user and password fields are empty. The ACAP-IP describes the IP address of the ACAP. The IG-ID is an identifier for the IG used in case there are multiple instances; it is fixed for a given IG and is used by the corresponding ACAP to identify the source of the message. The “reqType” field holds information on the message format used. The web client then dispatches the alert via HTTP.

5.1.1 **Database**

The web server and the IG main process have both accesses to a PostgreSQL database. The database includes five tables which are described in Table 5-1.

Table 5-1: IG database tables

Table name	Description	Fields of the table
area	Holds information on the	• Geocode

	area. Is used to map geo-codes to polygons and vice versa. The database is filled with data from all municipalities of the Catalan region (Spain) as preparation for the pilot demonstration.	• Area description (human readable version) • Type (e.g. polygon) • Coordinates • Altitude • Ceiling
channels	Holds information on the channels available.	• Channel Identifier (ID) • Channel description (human readable version) • Sent (number of sent messages) • Successful (number of successfully transmitted messages) • Rating (good, low, medium)
message_content	This table stores the sent message in human-readable version. To identify the corresponding CAP file, the incident and message ID is also stored.	• Incident ID • Message ID • Content
message_log	Stores all relevant data for an alert message.	• Incident ID • Message ID • Timestamp • Status (true if alert was dispatched) • Headline • Channels (list of acknowledgements) • Expires (expire field of the CAP file)
Subscriber_data	Holds the information of subscribers.	• ID • Name • Email address

5.1.2 **Alerting Services Web Services Specification**

This section gives the specification of the web services between the GUI and the IG.

The structuring of the methods is divided into HTTP-POST requests and HTTP-GET requests.

The web services provide the GUI with methods to create and manipulate alert messages at the IG. It is implemented by a PHP7 script running on the Linux machine with Apache2.

5.1.2.1 POST Methods

The POST methods URLs have the following structure:

```
http://<<IP>>/IG/<<postCommand>>
```

where <<IP>> is to be replaced by the IP address of the dedicated IG. Table 5-2 shows the commands that can be used with a POST request.

Table 5-2: HTTP POST commands of the IG web services

postCommand	**Description**

set	With set commands a CAP can be generated and values in this CAP can be set.
dispatch	Dispatches an alert message to the ACAPs
reset	Reset of different values in the CAP

Output is either and error message with HTTP status code 400 in the form of:

```
{
 "errormessage": <<error message>>,
}
```

Or upon success a message with HTTP status code 200 with the JSON encoded content described in the output field in the tables below. If the output is an alert message it is defined as:

```
{
 "header": <<headline of the alert message>>,
 "content": <<content of the alert message>>,
 "complete": <<array with all cap fields that are missing>>,
 "freeText": <<flag that indicates if there is free text in the message>>
}
```

The free text flag is needed at the receiver to determine whether a message can be automatically translated using the MCE or not. Input variables are sent in the HTTP POST message body in JSON format. For all POST commands the same body structure is used. It consists of the incident ID, the message ID, a field called *selectedItem* and a field called *itemValue*. An example for the JSON body is:

```
{
 "incidentId": "INC201529100941",
 "messageId": "1234567890",
 "selectedItem": "event",
 "itemValue": "Forest Fire,
 "language": "en-GB"
}
```

For the incidentId and the messageId field any value is possible except “null” which throws an error message. With the selectedItem field it is determined which part of the CAP is changed. The itemValue field is the value that shall be set. In some commands the itemValue field can be empty. In Table 5-3 and Table 5-4 the possible values of the selectedItem field are presented for the set command, in Table 5-5 for the dispatch command, and in Table 5-6 the ones for the rest command, respectively. In Table 5-3 the **M** column shows the mandatory fields that have to be set in order to prepare a complete CAP message. If the check box is selected it means it is a mandatory field. The language of the input JSON can be any value but if the language is not available at the IG it is set to “en-GB” by default.

Table 5-3: IG POST body values for the set command

Service	M	Description	Input	Output

ID					
	☐		**selectedItem**	**itemValue**	
IG_Set_1	☒	Set the message type	msgType	“Standard” or “Cancellation” or “Release”	Alert message
IG_Set_2	☒	Set the event field	event	Earthquake, Heavy rain, Flood, Explosion, Terrorist attack, Forest Fire, Train crash, Traffic Accident , Toxic Cloud, “Free Text” as string	Alert message
IG_Set_3	☒	Set the severity field	severity	Extreme, Severe, Moderate, Minor, Unknown, “Free Text” as string	Alert message
IG_Set_4	☒	Set the certainty field	certainty	Observed, Likely, Possible, Unlikely, Unknown	Alert message
IG_Set_5	☐	Set the instruction field	instruction	Free text	Alert message
IG_Set_6	☒	Set the scope of the message	scope	“Public” or “Private”	Alert message
IG_Set_7	☒	Set the response type	responseType	Shelter, Evacuate, Prepare, Execute, Monitor, None	Alert message
IG_Set_8	☒	Set the urgency field	urgency	Immediate, Expected, Future, Past, Unknown, None	Alert message
IG_Set_9	☐	Add a Language	language	{ “language”: ”STRING”, “headline”: ”STRING” “content”: “STRING”	Alert message

				}	
IG_Set_10	☐	Add a URI	uri	URI as string	Alert message
IG_Set_11	☒	Set the date	onsetDate	“DD:MM:YYYY;hh:mm"	Alert message
IG_Set_12	☐	Set the expiration date of the message	expirationDate	“DD:MM:YYYY;hh:mm"	Alert message

IG_Set_13	☒	Sets the area of to alert.	area	{
				“geocodes”: ”STRING separated by comma if multiple”
				}
				or
				{
				“circleDesc”: “STRING”,
				“circle”: ”WGS84 coordinate pair followed by a space character and a radius value in kilometres”
				}
				or
				{
				“polyDesc”: “STRING”,
				“polygon”: ” whitespace-delimited list of WGS 84 coordinate pairs”
				}
				Or any combination of the above three options.
					Alert message

IG_Set_14	☐	Set the addresses in case of a private message this is mandatory.	addresses	Addresses as string. Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.	Alert message
IG_Set_15	☒	Identifies the sender of the message	sender	sender as string	Alert message
IG_Set_16	☐	Sets the web page	web	String if not set default page is used	Alert message
IG_Set_17	☐	Channels for the transmission can be selected. All available are used as default	channels	Channels as string separated by comma Possible values TBD	Alert message

One exception from the POST request structure above is the Service IG_Set_18. This service is for uploading a file. Since files can be received from different sources the base64 formatting was shifted to the IG. Files are sent uncoded to the IG. With this, the HTTP body

is occupied by the file which is sent in content type multipart/form. The URL for this function is given by:

http://<<IP>>/IG/addFile/<<lang>>/<<incidentId>>:<<messageId>>

Table 5-4: IG POST body values for the add file command

Service ID	Description	Input	Output
IG_Set_18	A file is attached	File in post body	"ack": Acknowledgement (filename)

Table 5-5: IG POST body values for the dispatch command

Service ID	Description	Input		Output
		selectedItem	**itemValue**	
IG_Send_1	The message is dispatched via the ACAPs	empty	empty	"ack": Acknowledgement (alert message)

Table 5-6 IG POST body values for the reset command

Service ID	Description	Input		Output
		selectedItem	**itemValue**	
IG_Rst_1	Resets all fields besides: identifier, incidents, status, msgType, areaDesc	reset	empty	Alert message
IG_Rst_2	A, in a previous attached step, additional language field is removed.	removeLanguage	Language code	"ack": Acknowledgement (message that can be shown to the user)
IG_Rst_3	A, in a previous attached step, resource is removed.	removeResource		"ack": Acknowledgement (message that can be shown to the user)
IG_Rst_4	A list with message IDs given for an incident ID is send. A combined cancellation message is dispatched.	cancelmessageID	TBD	"ack": Acknowledgement (message that can be shown to the user with the list of cancelled messages)

5.1.2.2 GET Methods

In GET requests the variables required are URL encoded. They are either the incident ID and the message ID or only the incident ID. Like the POST commands, GET requests have always a main command word in the URL. For the GET requests these commands are shown in Table 5-7. Below, GET commands for filtering are presented. These can be used to access the IG alerting database. The URL of GET requests are the following:

http://<<IP>>/IG/<<getCommand>>/<<lang>>/<<incidentId:messageId>>

where <<id>> in the URL shall be set to <<incident:messageId>> for commands all commands not including the filter keyword and to <<incidentId>> for commands including the filter keyword. The <<getCommand>> needs to be replaced with a value from **Table 5-7** in the column getCommand in order to call the dedicated method.

Table 5-7: HTTP GET commands of the IG web services

Service ID	Description	getCommand	Output
IG_Show_3	Returns the message and the indicators if the message is complete or contains free text	checkMessage	Alert message

IG_Show_4	Returns an JSON encoded array with n messages that fit the input incident ID	filter/all	{
			"incidentId": incidentId
			"message":[n]
			}
			Where a “message” array is:
			"messageId": messageId,
			"date": timestamp,
			"time": timestamp,
			“status”: status,
			"headline": headline
			
			The status field hold if the message has be sent or only stored

IG_Show_5	Returns a JSON encoded array with n messages that fit the input incident ID and have been sent.	filter/sent	{
			"incidentId": incidentId
			"message":[n]
			}
			Where a “message” array is:
			"messageId": messageId,
			"date": timestamp,
			"time": timestamp,
			“status”: status,
			"headline": headline
			
			The status field hold if the message has be sent or only stored

IG_Show_6	Returns a JSON encoded array with n messages that fit the input incident ID and that have not sent but are stored by the system.	filter/stored	{
			"incidentId": incidentId
			"message":[n]
			}
			Where a “message” array is:
			"messageId": messageId,
			"date": timestamp,
			"time": timestamp,
			“status”: status,

			"headline": headline The status field hold if the message has be sent or only stored

IG_Show_7	Returns a JSON encoded array with ***n*** messages that fit the input incident ID or were cancelled	filter/cancelled	{
			"incidentId": incidentId
			"message":[n]
			}
			where a “message” array is:
			"messageId": messageId,
			"date": timestamp,
			"time": timestamp,
			“status”: status,
			"headline": headline
			
			The status field hold if the message has be sent or only stored

IG_Show_8	Returns a JSON encoded array with ***n*** messages that fit the input incident ID or were not cancelled	filter/notCancelled	{
			"incidentId": incidentId
			"message":[n]
			}
			Where a “message” array is:
			"messageId": messageId,
			"date": timestamp,
			"time": timestamp,
			“status”: status,
			"headline": headline
			
			The status field hold if the message has be sent or only stored

IG_Show_9	Returns the cap message (xml), for testing.	getCap	CAP message in XML

5.1.3 **First Responders Information Web Services Specification**

The first responder information service will be based on output from deliverable D6.7 Situation report and accordingly will be based on EDXL-SitRep. The specification for this will start after the first validation of the impact summary generation module at release B.

6 Test Plan

6.1.1 IG Verification

The IG can be tested by connecting it to the web-based GUI or by directly calling its web services with a REST client as test receiver to verify the correct transmission of alert messages. For all web services defined in Section 5.1.2 a test was performed using a correct and an incorrect input. In the *correct* case, the IG shall perform the specified action and return the specified reply. In the *incorrect* case, the IG shall reply with the specified error message.

A receiver app from previous project is used for the first tests. The HEIMDALL receiver app will be used as soon as the alert receiver is implemented.

Test ID	*TS_IG_01*
Requirements to be verified	• TR_Com_1 • TR_Com_2
Test objective	To verify that the IG is able to keep the population informed.
Test procedure	1. The user creates an alert message using the GUI 2. The user dispatches the created alert message 3. Alert is shown at the receiver application
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • Receiver application connected to the HEIMDALL system • GUI connected to the HEIMDALL system
Success criteria	Correct alert message received at the receiver application
Results analysis	*The test has been performed using a receiver application in a lab environment. Nevertheless, the app has the potential to be used as a receiver for the public.*
Success	Passed

Test ID	*TS_IG_02*
Requirements to be verified	• TR_Com_3
Test objective	To verify that the IG is able to create alert messages.
Test procedure	1. The user starts the alert creating wizard using the GUI 2. The user creates an alert message following the wizard
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • GUI connected to the HEIMDALL system
Success criteria	Correct alert message according to CAP is created.
Results analysis	*The created CAP file has been verified using an online CAP verification tool.*
Success	Passed

Test ID	*TS_IG_03*
Requirements to	• TR_Com_4

be verified	
Test objective	To verify that the IG is able to give access to users in the field.
Test procedure	1. A user connects to the system using the smartphone application. 2. The user requests specific data sets or an overview
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • Smartphone with HEIMDALL App installed connected to the HEIMDALL system.
Success criteria	The user can access the requested data.
Results analysis	-
Success	To be tested

Test ID	*TS_IG_04*
Requirements to be verified	• TR_Com_5
Test objective	To verify that the IG is able to consider access rights.
Test procedure	1. A user connects to the system using the smartphone application using credentials that give him full access. 2. The user requests specific data sets or an overview
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • Smartphone with HEIMDALL App installed connected to the HEIMDALL system.
Success criteria	The user can access the requested data.
Results analysis	-
Success	To be tested

Test ID	*TS_IG_05*
Requirements to be verified	• TR_Com_5
Test objective	To verify that the IG is able to give access to users in the field.
Test procedure	1. A user connects to the system using the smartphone application using credentials that give him no access. 2. The user requests specific data sets or an overview
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • Smartphone with HEIMDALL App installed connected to the HEIMDALL system.
Success criteria	The user cannot access the requested data.
Results analysis	-
Success	To be tested

Test ID	*TS_IG_06*

Requirements to be verified	• TR_Com_5
Test objective	To verify that the IG is able to give access to users in the field.
Test procedure	1. A user connects to the system using the smartphone application using credentials that give him only partial access. 2. The user requests specific data sets or an overview
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • Smartphone with HEIMDALL App installed connected to the HEIMDALL system.
Success criteria	The user can access the requested data where he is allowed to access it.
Results analysis	-
Success	To be tested

Test ID	*TS_IG_07*
Requirements to be verified	• TR_Com_14
Test objective	To verify that the IG is able to consider predefined areas of different levels
Test procedure	1. An alert message is created and different levels of areas are selected at the GUI
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • GUI connected to the HEIMDALL system
Success criteria	Areas of all levels are updated accordingly at the alert message
Results analysis	-
Success	To be tested

Test ID	*TS_IG_08*
Requirements to be verified	• TR_Com_15
Test objective	To verify that the IG is able to consider predefined areas of different levels
Test procedure	1. An alert message is created and types of areas are selected at the GUI
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • GUI connected to the HEIMDALL system
Success criteria	Areas of different types are updated accordingly at the alert message
Results analysis	*The IG showed the potential to work with different areas. The areas however need to be read from the SP in order to offer it for a larger scale of service.*
Success	Passed

Test ID	*TS_IG_09*
Requirements to	• TR_Com_16

be verified	
Test objective	To verify that the IG is able to consider different types of users as recipients within the private message
Test procedure	1. An alert message is created and as scope private is selected. 2. Using the set addresses method different user groups according to CAP are set
Test prerequisites/ configuration	• IG connected to the HEIMDALL system • GUI connected to the HEIMDALL system
Success criteria	The groups are updated accordingly at the alert message and the message is set to private
Results analysis	*The tested fields are free text so all kind of users can be included. It might be beneficial to have a set of predefined values for usability.*
Success	Passed

Test ID	*TS_IG_09*
Requirements to be verified	• TR_Com_17
Test objective	To verify that the IG is able to consider different types of users as recipients within the private message
Test procedure	1. An alert message is created 2. Using the set channel method different channels are selected 3. The message is dispatched
Test prerequisites/ configuration	• IG up and running
Success criteria	The channels files at the IG are updated and in case of dispatch the IG forwards the message to the dedicated channels.
Results analysis	-
Success	To be tested

Test ID	*TS_IG_10*
Requirements to be verified	• TR_Com_11 • TR_Com_12
Test objective	To verify that the IG is able to connect communication networks.
Test procedure	1. The machine of the IG connects to the HEIMDALL VPN 2. Test requests are send from SP side to the IG.
Test prerequisites/ configuration	• Machine of the IG is up and running
Success criteria	The SP and the IG can exchange data.
Results analysis	*The machine can connect to communication networks*
Success	Passed

Test ID	*TS_IG_11*
Requirements to be verified	• TR_Com_21
Test objective	To verify that the IG is able to share pictures
Test procedure	4. An alert message is created 5. Using the add file method a picture file is attached to the message 6. The message is dispatched
Test prerequisites/ configuration	• IG up and running
Success criteria	The message is forwarded including the picture
Results analysis	*The file was added using a test function.*
Success	Passed

7 Conclusion

This document presented the design and implementation status of the information gateway and satellite communication modules, being developed for the HEIMDALL platform. Requirements and implementation status of the HEIMDALL smartphone application is presented as well in the interim. The TRs presented here include the user feedback and suggestions collected during the initial 18 months of the project. An initial version of the IG functionalities developed for Release-A has been successfully integrated and tested as part of the corresponding end user workshop (EUW2, M18). Further development of the IG is ongoing as part of the upcoming releases of the HEIMDALL platform. The portable satellite terminal will be acquired at a later stage and in turn commissioned. It will be eventually tested in the second part of year 2019 in view of its final use at the final demo of the project in March' 20 in Catalunia.

8 References

[1] Alert4All: Alert for all, available at: https://cordis.europa.eu/project/rcn/98427/factsheet/en [last accessed Feb. 2019]

[2] PHAROS: *Project on a multi-hazard open platform for satellite based downstream services* available at https://cordis.europa.eu/project/rcn/188829/reporting/en [last accessed Feb. 2019]

[3] OASIS Standard, Common Alerting Protocol Version 1.2 available at http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html [last accessed Feb. 2019]

[4] Barth, B. (2017), HEIMDALL D2.6: HEIMDALL Requirements Report – Issue 1

[5] Barth, B. (2019), HEIMDALL D2.7: HEIMDALL Requirements Report – Issue 2

[6] To be released in M38 (2020), HEIMDALL D5.7: First Responders Data Module Design

[7] To be released in M38 (2020), HEIMDALL D4.17: Communication to Remote Areas – Design and Specifications – Final

End of document