



Driving Innovation in Crisis Management  
for European Resilience



## D934.32 SOLUTION SCENARIOS AND INTEGRATION TEST RESULTS V2

SP93 - SOLUTIONS

DECEMBER 2019 (M68)



This project has received funding from the European Union's 7th Framework Programme for Research, Technological Development and Demonstration under Grant Agreement (GA) N° #607798

## Project information

<b>Project Acronym:</b>	DRIVER+
<b>Project Full Title:</b>	Driving Innovation in Crisis Management for European Resilience
<b>Grant Agreement:</b>	607798
<b>Project Duration:</b>	72 months (May 2014 - April 2020)
<b>Project Technical Coordinator:</b>	TNO
<b>Contact:</b>	<a href="mailto:coordination@projectdriver.eu">coordination@projectdriver.eu</a>

## Deliverable information

<b>Deliverable Status:</b>	Final
<b>Deliverable Title:</b>	D934.32 Solution scenarios and integration test results v2
<b>Deliverable Nature:</b>	Report (R)
<b>Dissemination Level:</b>	Public (PU)
<b>Due Date:</b>	December 2019 (M68)
<b>Submission Date:</b>	20/12/2019
<b>Subproject (SP):</b>	SP93 - Solutions
<b>Work Package (WP):</b>	WP934 - DRIVER+ CM Solutions
<b>Deliverable Leader:</b>	FRQ, Ludwig Kastner
<b>Reviewers:</b>	Gerald Schimak, AIT Maurice Sammels, XVR Hector Naranjo, GMV
<b>File Name:</b>	DRIVER+_D934.32_Solution scenarios and integration test results v2.docx
<b>Version of template used:</b>	V2.2 – February 2019

### DISCLAIMER

The opinion stated in this report reflects the opinion of the authors and not the opinion of the European Commission. All intellectual property rights are owned by the DRIVER+ consortium members and are protected by the applicable laws. Except where otherwise specified, all document contents are: "©DRIVER+ Project - All rights reserved". Reproduction is not authorised without prior written agreement.

The commercial use of any information contained in this document may require a license from the owner of that information.

All DRIVER+ consortium members are also committed to publish accurate and up to date information and take the greatest care to do so. However, the DRIVER+ consortium members cannot accept liability for any inaccuracies or omissions nor do they accept liability for any direct, indirect, special, consequential or other losses or damages of any kind arising out of the use of this information.

## Revision Table

Issue	Date	Comment	Author
V0.01	05/12/2018	Initial TOC and draft content	Ludwig Kastner, FRQ, Task Leader
V0.02	12/12/2018	Creation of sections 2.3, 2.4 and 2.5 based on integration test reports from Trial 1 preparations	Ludwig Kastner, FRQ, Task Leader
V0.03	19/12/2018	Updating to the new template and merging content from different versions	Ludwig Kastner, FRQ, Task Leader
V0.04	07/01/2019	Adding information from mail conversations with solution providers	Ludwig Kastner, FRQ, Task Leader
V0.05	14/01/2019	Adding information from mail conversations with solution providers	Ludwig Kastner, FRQ, Task Leader
V0.06	14/03/2019	Adding information from mail conversations with solution providers	Ludwig Kastner, FRQ, Task Leader
V0.07	14/05/2019	Adding information from mail conversations with solution providers	Ludwig Kastner, FRQ, Task Leader
V0.08	07/2019	Collecting Information from Trial 4 execution, taking into account After-Action Review Tool recordings	Hubert König, FRQ
V0.09	08/2019	Consolidating Information from Trial 3 and 4	Ludwig Kastner, Hubert König, FRQ
V0.10	08/2019	Inputs for section 6, integration of internal, non-selected solutions. Inputs for section 7, Technical integration efforts.	Andrzej Adamczyk, ITTI Antonio Chagas, EdiSoft Joachim Klerx, Daniel Auferbauer, Sebastian Sippl, AIT Aurélie Montarnal, Armines Christian Niermann, DLR Michael Middelhoff, WWU Eelco Narding, SIM-CI Govert ter Mors, Nelen-Schuurmans Vincent Pourieux, VWORLD Håkon Eggemoen, AnsuR Ruud van den Beukel, Merlin
V0.11	06/09/2019	Version for preliminary internal review (mainly concerning Trial 4)	Hubert König, FRQ
V0.12	26/09/2019	Incorporated Review Comments from Gerhard Zuba regarding Trial 4; Added swim lane diagrams for Trial 3 use cases. Added Partner contribution to section 7	Hubert König, FRQ

Issue	Date	Comment	Author
V0.13	15/10/2019	Consolidating Information from Trial 3. Version for preliminary internal review of Trial 3 section.	Ludwig Kastner, Hubert König, FRQ
V0.14	23/10/2019	Incorporated Review Comments from Gerhard Zuba regarding Trial 3. Inserted References. Applied newest document template. Initial information from Final Demo.	Hubert König, FRQ
V0.15	25/10/2019	Information added on Trial independent Test-bed integration of internal non-selected solutions.	Ludwig Kastner, Hubert König, FRQ
V0.16	28/10/2019	Initial Review	Gerald Schimak, AIT
V0.17	28/10/2019	Review of Sections 1, 2 and 3	Dražen Ignjatović, AIT
V0.18	21/11/2019	Peer Review	Hector Naranjo, GMV
V0.19	22/11/2019	Peer Review	Maurice Sammels, XVR
V0.20	07/12/2019	Modifications according to peer review comments; Completion of Final Demo section.	Ludwig Kastner, Hubert König, FRQ Bernard Stepien, Creotech Vincent Pourieux, VWORLD Raúl Valencia Pérez, GMV Daniele Galliano, JRC
V0.21	10/12/2019	Modifications in Executive Summary and Conclusions sections. Added “Considerations for future test and integration activities” section.	Ludwig Kastner, FRQ Todor Tagarev, Petya Ivanova, Valeri Ratchev, CSDM Laurent Dubost, Cyril Dangerville, TCS Hubert König, FRQ (ed.)
V0.22	17/12/2019	Final Review	Gerald Schimak, AIT, Dražen Ignjatović AIT, Hector Naranjo GMV, Maurice Sammels XVR and Alexander Scharnweber DLR
V0.23	19/12/2019	Final Changes	Ludwig Kastner, FRQ Hubert König, FRQ (ed.)
V0.24	20/12/2019	Final check and approval for submission	Tim Stelkens-Kobsch, DLR, Quality Manager
V0.25	20/12/2019	Final check and approval for submission	Marijn Rijken, TNO, Project Director
V1.0	20/12/2019	Final check and submission to the EC	Francisco Gala, ATOS

## The DRIVER+ project

---

Current and future challenges, due to increasingly severe consequences of natural disasters and terrorist threats, require the development and uptake of innovative solutions that are addressing the operational needs of practitioners dealing with Crisis Management. DRIVER+ (Driving Innovation in Crisis Management for European Resilience) is an FP7 Crisis Management demonstration project aiming at improving the way capability development and innovation management is tackled. DRIVER+ has three main objectives:

1. Develop a pan-European Test-bed for Crisis Management capability development:
  - a. Develop a common guidance methodology and tool, supporting Trials and the gathering of lessons learnt.
  - b. Develop an infrastructure to create relevant environments, for enabling the trialling of new solutions and to explore and share Crisis Management capabilities.
  - c. Run Trials in order to assess the value of solutions addressing specific needs using guidance and infrastructure.
  - d. Ensure the sustainability of the pan-European Test-bed.
2. Develop a well-balanced comprehensive Portfolio of Crisis Management solutions:
  - a. Facilitate the usage of the Portfolio of solutions.
  - b. Ensure the sustainability of the Portfolio of solutions.
3. Facilitate a shared understanding of Crisis Management across Europe:
  - a. Establish a common background.
  - b. Cooperate with external partners in joint Trials.
  - c. Disseminate project results.

In order to achieve these objectives, five Subprojects (SPs) have been established. **SP91 Project Management** is devoted to consortium level project management, and it is also in charge of the alignment of DRIVER+ with external initiatives on Crisis Management for the benefit of DRIVER+ and its stakeholders. In DRIVER+, all activities related to Societal Impact Assessment are part of **SP91** as well. **SP92 Test-bed** will deliver a guidance methodology and guidance tool supporting the design, conduct and analysis of Trials and will develop a reference implementation of the Test-bed. It will also create the scenario simulation capability to support execution of the Trials. **SP93 Solutions** will deliver the Portfolio of solutions which is a database driven web site that documents all the available DRIVER+ solutions, as well as solutions from external organisations. Adapting solutions to fit the needs addressed in Trials will be done in **SP93**. **SP94 Trials** will organise four series of Trials as well as the Final Demo (FD). **SP95 Impact, Engagement and Sustainability**, is in charge of communication and dissemination, and also addresses issues related to improving sustainability, market aspects of solutions, and standardisation.

The DRIVER+ Trials and the Final Demonstration will benefit from the DRIVER+ Test-bed, providing the technological infrastructure, the necessary supporting methodology and adequate support tools to prepare, conduct and evaluate the Trials. All results from the Trials will be stored and made available in the Portfolio of solutions, being a central platform to present innovative solutions from consortium partners and third parties, and to share experiences and best practices with respect to their application. In order to enhance the current European cooperation framework within the Crisis Management domain and to facilitate a shared understanding of Crisis Management across Europe, DRIVER+ will carry out a wide range of activities. Most important will be to build and structure a dedicated Community of Practice in Crisis Management, thereby connecting and fostering the exchange of lessons learnt and best practices between Crisis Management practitioners as well as technological solution providers.

## Executive summary

---

This document describes the main activities related to the integration of solutions into the Test-bed, focusing on the adaptations and integration activities which were required to prepare the solutions for Trial 3, Trial 4 and the Final Demo. The corresponding activities performed for Trial 1 and Trial 2 were reported in deliverable **D934.31 DRIVER+ solution Scenarios and integration test results V1** (1).

Overall target for solution integration is to increase the efficiency and effectiveness of modern Crisis Management. It shall enable an automated exchange of data between different IT solutions in order to achieve the following:

- Less time needed for practitioners in their search for crisis relevant information.
- More comfort for practitioners to find relevant information due to optimized presentation of information (e.g. by using user interfaces which are familiar to them)
- Less time needed for practitioners to read data from one solution and entering data manually into another solution.
- Lower probability for wrong information caused by human errors while reading/entering data from/into a solution.
- More time left for practitioners to analyse and interpret the information and to define, communicate, execute and supervise crisis response actions.
- Higher quality of the Crisis Management outcome due to time savings, better data quality and improvements in crisis relevant communication.

As a starting point into this direction, user needs currently not fulfilled by legacy IT systems are described in the DRIVER+ project in form of “Crisis Management gaps”, see (2). These gaps are the basis for the creation of the Trial scenarios which form the basis for the underlying test cases. The effort to design, prepare and finally perform these test cases for solution interaction from a technical point of view is reported in this document. The final achievements for Trial 3, 4 and the Final Demo regarding how the selected solutions and the solution integration could fill the gaps are described in the Trial Evaluation reports (3), (4) and (5).

The document starts by providing a brief overview of the Test-bed and its role for solution integration, followed by a general introduction to the solution integration process. The challenges of Trial 3, 4 and the Final Demo from a technical integration perspective were mainly the involvement of external solution providers in a complex scenario and the Trial execution with the interaction of these solutions. External solution providers had to develop an understanding of the DRIVER+ integration and Test-bed concept. The selected solutions are described with a focus on their integration and adaptation efforts which were necessary in order to best support the Trial scenarios. Each Trial execution had one preceding technical integration meeting and two preceding Dry Runs which turned out to be absolutely necessary in order to prepare the Trials properly, both from a technical and an organizational perspective.

Having all DRIVER+ internal solutions integrated in the Test-bed provides advantages such as a more comprehensive Test-bed and a good preparation for any future integration work for the period when the Test-bed will be used beyond the end of the project. Thus, this document also describes the “Trial independent Test-bed integration” of internal solutions as for all remaining DRIVER+ internal solutions which were not selected for Trials a similar path was followed to integrate them into the Test-bed. For this category of solutions separate use-cases were introduced. These use-cases and related test cases were necessary in order to properly test the integration of those solutions into the Test-bed. The achievement of a successful integration contributes to the sustainability of the DRIVER+ project.

Finally, the document closes with a section about considerations for future test and integration activities of Crisis Management solutions highlighting additional aspects relevant for an introduction of new IT solution before they can be used in an operational environment.

## TABLE OF CONTENT

---

1.	Introduction.....	20
1.1	Identification of intended audience.....	20
1.2	Scope of the document .....	20
1.3	Document structure .....	20
2.	Solution integration process through the Test-bed.....	21
2.1	Solution integration process.....	21
2.2	Solution integration events .....	22
2.3	Brief description of the Test-bed .....	22
2.3.1	Test-bed components .....	23
2.4	Solution integration information and support .....	24
3.	Trial 3 .....	26
3.1	CM gaps covered in Trial 3 .....	26
3.2	Scenario description of Trial 3 .....	27
3.3	Participating solutions.....	28
3.4	Trial 3 intended solution interaction.....	29
3.5	Trial preparation and execution .....	31
3.5.1	Overview .....	31
3.5.2	Use cases .....	31
3.5.3	Test cases .....	34
3.5.4	Solution integration results .....	36
3.6	Solution providers' adaptations and integration technical details .....	38
3.6.1	ASIGN .....	38
3.6.2	viewTerra Evolution.....	39
3.6.3	CrowdTasker .....	40
3.6.4	Airborne and Terrestrial Situational Awareness.....	42
4.	Trial 4 .....	46



4.1	CM gaps addressed in Trial 4 .....	46
4.2	Scenario description of Trial 4 .....	47
4.3	Participating solutions.....	47
4.4	Trial 4 intended solution interaction.....	50
4.5	Trial preparation and execution .....	51
4.5.1	Overview .....	51
4.5.2	Use cases .....	53
4.5.3	Test cases .....	58
4.5.4	Solution integration results .....	59
4.6	Solution providers' adaptations and integration technical details .....	62
4.6.1	Airborne and Terrestrial Situational Awareness.....	63
4.6.2	HumLogSIM .....	65
4.6.3	3Di .....	65
4.6.4	SIM-CI .....	66
4.6.5	CrisisSuite .....	68
4.6.6	LCMS.....	68
5.	Final Demo .....	70
5.1	CM gaps addressed in the Final Demonstration .....	70
5.2	Scenario description.....	71
5.3	Participating solutions.....	71
5.4	Final Demo intended solution interaction .....	72
5.5	Final Demo preparation and execution.....	73
5.5.1	Overview .....	73
5.5.2	Use cases .....	74
5.5.3	Test cases .....	75
5.5.4	Solution integration results .....	76
5.6	Solution providers' adaptations and integration technical details .....	80
5.6.1	CrisisSuite .....	80



5.6.2	SOCRATES OC.....	80
5.6.3	vieWTerra Evolution.....	81
5.6.4	Drone Rapid Mapping .....	83
5.6.5	Field Reporting Tool .....	84
6.	Trial independent Test-bed integration of internal (non-selected) solutions.....	85
6.1	DRIVER+ solution categorisation .....	85
6.2	Solutions integration overview .....	85
6.3	Solution integration achievements .....	86
6.3.1	Rumour Debunker.....	87
6.3.2	Protect.....	89
6.3.3	IO-DA.....	90
6.3.4	EMT (Emergency Map Tool) .....	91
6.3.5	PROceed Laboratory .....	91
7.	Considerations for future test and integration activities of Crisis Management solutions .....	93
7.1	Objectives and methodological approach .....	93
7.2	Technology-based classification of solutions .....	94
7.3	Types of potential safety and security impact of CM solutions.....	95
7.4	Pertinent “Technology-Impact” combinations .....	96
7.5	Sample safety and security norms for pertinent “Technology-Impact” combinations.....	98
7.6	Illustrative test cases .....	98
7.7	Implementation .....	98
8.	Conclusions.....	99
	References.....	101
	Annex 1 – DRIVER+ Terminology.....	103
	Annex 2 – Trial 3 – Technical details.....	105
	Annex 3 – Trial 4 – Technical details.....	113
	Annex 4 – Final Demonstration – Technical details.....	121
	Annex 5 – Integration reports of non-selected internal solutions .....	126

A5.1 Rumour Debunker .....	126
A5.2 Protect .....	129
A5.3 IO-DA .....	136
A5.4 PROCEED Laboratory .....	142
Annex 6 – Sample safety and security norms for pertinent “Technology-Impact” combinations.....	144
Annex 7 – Illustrative test cases .....	161
Test Case 1 “Personal Data Protection in the Social Media Analysis Platform” .....	161
Test Case 2 “Providing confidentiality, integrity and availability of information in CrisisSuite” .....	161
Test Case 3 “Security of digital infrastructure in the Common Information Space” .....	162

## List of Figures

---

Figure 2.1: DRIVER+ solution integration process .....	21
Figure 2.2: The Test-bed and its components .....	23
Figure 3.1: Trial 3 solution interactions .....	30
Figure 3.2: Solution interaction diagram for Trial 3 .....	31
Figure 3.3: Interaction sequence diagram for the Situation Assessment phase (sub-scenario #2) .....	33
Figure 3.4: Interaction sequence diagram for the Confirmation phase (sub-scenario #3).....	33
Figure 3.5: Interaction sequence diagram for sub-scenario #4a (Chemical spill) .....	34
Figure 3.6: Interaction sequence diagram for Communication phase (sub-scenario #5).....	34
Figure 3.7: Overall information flow sequence diagram for Trial 3 .....	36
Figure 3.8: Sequence Diagram for the ASIGN to Test-bed Photo and Mission adapters.....	38
Figure 3.9: viewWTerra Evolution example screenshot .....	40
Figure 3.10: Mission planning capabilities in U-Fly .....	42
Figure 3.11: Generated digital surface model (DSM) .....	43
Figure 3.12: Pre- and post-disaster landslide.....	44
Figure 3.13: Mosaic with 15 cm resolution .....	44
Figure 3.14: Plotted 2D map product .....	45
Figure 4.1: Trial 4 solution interactions .....	50
Figure 4.2: Information exchange diagram for the Trial 4 solutions .....	51
Figure 4.3: Trial 4 data exchange via Test-bed .....	52
Figure 4.4: Trial 4 data flow within the Test-bed .....	52

Figure 4.5: Use case: Sim-CI – Publish Info (electricity, drinking water, telecom, traffic congestion, vulnerable buildings) .....	54
Figure 4.6: Use case: 3Di – Publish flood map prediction.....	54
Figure 4.7: Use case: CrisisSuite – Publish map layers.....	55
Figure 4.8: Use case: CrisisSuite – Publish summary/overview .....	55
Figure 4.9: Use case: ZKI – Publish current flood map .....	56
Figure 4.10: Use case: HumLogSim – Assess/Update evacuation plan .....	56
Figure 4.11: Use case: LMCS – Publish map layers.....	57
Figure 4.12: Use case: LMCS – Publish summary/overview.....	57
Figure 4.13: Overall information flow sequence diagram for Trial 4.....	61
Figure 5.1: Final Demo solution interactions .....	73
Figure 5.2: solution interaction diagram for the Final Demo.....	74
Figure 5.3: Overall information flow sequence diagram for the Final Demo .....	77
Figure 6.1: Information Flow in the Rumour Debunker solution integration scenario .....	88
Figure 6.2: Sequence of information flow when visualising possible future situation (objects configuration) .....	92
Figure 7.1: Safety and security related testing of Crisis Management solutions: Methodological approach.	93
Figure A2.1: Data Exchange Diagram of Trial 3 .....	105
Figure A2.2: Physical deployment of solution back-ends for Trial 3 .....	106
Figure A2.3: Technical solution integration, using various topics configured in the Test-bed .....	107
Figure A2.4: Trial 3 – Sub-scenario #2 sequence diagram – example extract.....	108
Figure A2.5: Trial 3 – Sub-scenario #3 sequence diagram – example extract.....	109
Figure A2.6: Trial 3 – Sub-scenario #4a sequence diagram – example extract.....	110

Figure A2.7: Trial 3 – Sub-scenario #5 sequence diagram – example extract.....	111
Figure A3.1: Data Exchange Diagram of Trial 4 .....	113
Figure A3.2: Physical deployment of solution back-ends for Trial 4 .....	114
Figure A3.3: Technical solution integration, using various topics configured in the Test-bed .....	115
Figure A3.4: Trial 4 - Block 1 sequence diagram – example extract.....	116
Figure A3.5: Trial 4 - Block 2 sequence diagram – example extract.....	117
Figure A4.1: Data Exchange Diagram of the Final Demo .....	121
Figure A4.2: Physical deployment of solution back-ends for the Final Demo .....	122
Figure A4.3: Technical solution integration, using various topics configured in the Test-bed .....	123
Figure A4.4: Final Demo, Dry Run 2 example sequence diagram (extract) .....	124
Figure A5.5: Example Screenshot (Android App) .....	128
Figure A5.6: Docker Engine .....	129
Figure A5.7: Docker Engine (2) .....	129
Figure A5.8: Docker Engine (3) .....	130
Figure A5.9: Test bed version 1.2.8 jar .....	130
Figure A5.10: Protect .....	131
Figure A5.11: Protect Rest adapter End Point developed from the start.....	131
Figure A5.12: Result of the received message in the Test Bed .....	132
Figure A5.13: Result of the sent message in Protect Endpoint.....	132
Figure A5.14: Protect sending a EMSI message .....	133
Figure A5.15: Message sent from Protect and received in Test Bed.....	134
Figure A5.16: Doing a curl command with a EMSI message in the Test Bed .....	135

Figure A5.17: Received message in Protect End point .....	135
Figure A5.18: IO-DA's GIS completed with the risks sent into the CAP alert file from another solution .....	137
Figure A5.19: BPMN process deduced by IO-DA from the information available on the crisis in the database .....	137
Figure A5.20: BPMN process deduced by IO-DA from the information available on the crisis in the database .....	138
Figure A5.21: Initial state of the IO-DA GIS .....	139
Figure A5.22: CAP message sent to the Test-bed and received by IO-DA .....	139
Figure A5.23: The data has been successfully integrated into the knowledge base .....	140
Figure A5.24: Screenshot of the method called to send process to the Test-bed .....	141
Figure A5.25: file successfully sent to the Test-bed .....	141
Figure A5.26: PROCeed Laboratory screen – exporting objects .....	142
Figure A5.27: PFSP received by the Test-bed broker .....	143

## List of Tables

---

Table 2.1: Main components of the Test-bed .....	24
Table 3.1: Dates and locations of TIM, DR1, DR2 and Trial 3 execution .....	26
Table 3.2: Crisis Management high priority gaps covered in Trial 3 .....	26
Table 3.3: Selected solutions for Trial 3 .....	28
Table 3.4: Solutions overview for Trial 3 .....	29
Table 3.5: Trial 3 solution integration with Test-bed .....	30
Table 3.6: Use cases per sub-scenario in Trial 3 .....	32
Table 3.7: Test cases related to solution integration performed in Trial 3 DR1 and DR2 .....	35

Table 3.8: Test cases and test results achieved in DR1 and DR2 .....	37
Table 4.1: Dates and locations of DR1, DR2 and Trial 4 execution.....	46
Table 4.2: CM gaps addressed in Trial 4 .....	46
Table 4.3: Selected solutions for Trial 4.....	48
Table 4.4: Solutions overview for Trial 4.....	48
Table 4.5: Solution integration with Test-bed.....	50
Table 4.6: Use cases per solution in Trial 4 .....	53
Table 4.7: Test cases related to solution integration performed in Trial 4 DR1 and DR2.....	58
Table 4.8: Test cases and test results achieved in DR1 and DR2.....	62
Table 5.1: Dates and locations of TIM, DR1, DR2 and Final Demo .....	70
Table 5.2: CM gaps addressed in the Final Demo .....	70
Table 5.3: Selected solutions for the Final Demonstration.....	71
Table 5.4: Solutions overview for the Final Demonstration .....	71
Table 5.5: Solution integration with Test-bed.....	73
Table 5.6: Use of solutions in the Final Demo.....	74
Table 5.7: Final Demo solution integration test cases.....	75
Table 5.8: Test results achieved in DR1, DR2 and DR2½ of the Final Demo .....	78
Table 6.1: Selection of internal solutions for individual Trials / Final Demo .....	85
Table 6.2: Selection of external solutions for individual Trials / Final Demo.....	86
Table 7.1: Technology-Impact of combinations. ....	97
Table A1: DRIVER+ Terminology.....	103
Table A2.1: Trial 3 – LargeDataUpdate message example.....	111



Table A2.2: Trial 3 – FeatureCollection message example .....	112
Table A2.3: Trial 3 – MapLayerUpdate message example .....	112
Table A3.1: Trial 4 – LargeDataUpdate message example.....	118
Table A3.2: Trial 4 – Log message example .....	118
Table A3.3: Trial 4 – GeoJSON message example.....	119
Table A3.4: Trial 4 – Alert message example .....	120
Table A4.1: Final Demo – LargeDataUpdate message example.....	125
Table A4.2: Trial 4 – Alert message example .....	125

## List of Acronyms

Acronym	Definition
<b>AAR tool</b>	After-Action Review tool
<b>AIT</b>	Austrian Institute of Technology
<b>AMP</b>	Advanced Medical Post
<b>BPMN</b>	Business Process Model and Notation
<b>C3</b>	Command, Control, and Communication
<b>CAP</b>	Common Alerting Protocol, an XML-based data format for exchanging public warnings and emergencies between alerting technologies
<b>CBRN</b>	Chemical, Biological, Radiological, and Nuclear
<b>CEN</b>	European Committee for Standardization (French: Comité Européen de Normalisation)
<b>CfA</b>	Call for Application
<b>CIA</b>	Confidentiality, Integrity and Availability
<b>CIS</b>	Common Information Space
<b>COP</b>	Common Operational Picture
<b>CSDM</b>	Centre of Security and Defence Management
<b>CWA</b>	CEN Workshop Agreement
<b>DB</b>	Database
<b>DCP</b>	Data Collection Plan
<b>DoW</b>	Definition of Work
<b>DR1</b>	Dry Run 1
<b>DR2</b>	Dry Run 2
<b>EMSI</b>	Emergency Management Shared Information, an XML-based protocol for exchanging emergency management information between alerting technologies
<b>ERCC</b>	Emergency Response Coordination Centre
<b>ETSI</b>	European Telecommunications Standards Institute
<b>EUCP</b>	European Civil Protection
<b>EUCPM</b>	European Civil Protection Mechanism
<b>EUCPT</b>	EU Civil Protection Team
<b>FTP</b>	File Transfer Protocol
<b>GIS</b>	Geographic Information System
<b>GDPR</b>	General Data Protection Regulation
<b>HQ</b>	Head Quarters

Acronym	Definition
<b>HTM</b>	Haagse Tramweg Maatschappij (public transport)
<b>IASC</b>	Inter-Agency Standing Committee (of the UN)
<b>IC</b>	Incident Commander
<b>ICT</b>	Information and Communication Technology
<b>IEC</b>	International Electrotechnical Commission
<b>IM</b>	Incident Manager
<b>ITU</b>	International Telecommunication Union
<b>JSON</b>	JavaScript Object Notation
<b>KML/ KMZ</b>	Keyhole Markup Language
<b>LCMS</b>	Landelijk Crisis Management Systeem (Nationwide Crisis Management System of The Netherlands)
<b>MQ</b>	Message Queue
<b>N.A.</b>	Not Applicable
<b>NDMA</b>	National Disaster Management Agency
<b>ÖRK</b>	Österreichisches Rotes Kreuz (Austrian Red Cross)
<b>OST</b>	Observer Support Tool
<b>PFA</b>	Psychological First Aid
<b>PFSP</b>	Possible Future Situational Picture
<b>POI</b>	Point of Interest
<b>POK</b>	Partly O.K.
<b>PoS</b>	Portfolio of Solutions
<b>PSS</b>	PsychoSocial Support
<b>QGIS</b>	Quantum GIS (a free and open-source cross-platform geographic information system)
<b>REST</b>	Representational State Transfer
<b>ROI</b>	Region Of Interest
<b>RPAS</b>	Remotely Piloted Aerial System
<b>RPV</b>	Remotely Piloted Vehicle
<b>SiTac</b>	Situation Tactique (tactical situation)
<b>SitRep</b>	Situational Report
<b>SRH</b>	Safety Region Haaglanden
<b>Stedin</b>	Electricity provider (in The Hague)
<b>SW</b>	Software
<b>TGM</b>	Trial Guidance Methodology

Acronym	Definition
<b>THG</b>	City of The Hague
<b>TA</b>	Test Activity
<b>TC</b>	Test Case
<b>TCS</b>	Thales Communications & Security
<b>TIFF</b>	Tagged Image File Format
<b>TIM</b>	Technical Integration Meeting
<b>TMT</b>	Trial Management Tool
<b>TP</b>	Transit Point
<b>TR</b>	Test Report
<b>TS</b>	Test Scenario
<b>UAS</b>	Unmanned Aerial System
<b>UI</b>	User Interface
<b>UML</b>	Unified Modelling Language
<b>URL</b>	Uniform Resource Locator
<b>VM</b>	Virtual Machine
<b>WFS</b>	Web Feature Service
<b>WMS</b>	Web Mapping Service
<b>ZKI-Tool</b>	One of the modules of Airborne and Terrestrial Situation Awareness solution

## 1. Introduction

---

One of the main and implicit objectives of the DRIVER+ project is the sustainability of its outcome. The contribution of this deliverable to sustainability consists of documenting the experiences gained during the Trial preparations and executions from a technical perspective. The process of solution integration starts with the challenges of each Trial scenario and the ideas for automated data exchange among the solutions in order to support the work of the practitioners to the highest possible extent. The process to achieve this automated data exchange is described mainly at the technical level of solution integration including the related test and documentation effort.

### 1.1 Identification of intended audience

---

The intended audiences of this document are:

- Users who aim at preparing Trial activities beyond the end of the DRIVER+ project and want to learn from the integration efforts performed for Trial 3 and Trial 4.
- Solution providers who aim at integrating their solution into the Test-bed and who want to take advantage of lessons learned from previous integration efforts.
- Everyone who wants insight into the integration process of solutions.

### 1.2 Scope of the document

---

The scope of this document is to describe the integration of solutions into the Test-bed as well as the test scenarios needed to assess and evaluate the integration. The main scope of the document covers Trial-specific integrations but also the integration of solutions that were not part of any of the 4 Trials is covered in this document in a separate section.

Thus, the document shall give insight which technical efforts are required for preparing, testing and running a Trial, and what typically must be done for the integration of solutions into the Test-bed.

### 1.3 Document structure

---

The document starts with a short description of the solution Integration Process (including an overview of the Test-bed and its components) and continues by describing the work and results of the solution integration performed for Trial 3 (also called “Trial Austria”), Trial 4 (Trial “The Netherlands”) and the Final Demo (that took place in Poland and The Netherlands). For each of the Trials the document provides a short overview of the DRIVER+ solution scenarios and lists the preparation steps, especially their Dry Run 1 (DR1) and Dry Run 2 (DR2) events as they are most relevant for the solution integration work. Each of the three Trial-descriptions concludes with a description of adaptations that have been performed by the individual solution providers in order to integrate their solutions to the Test-bed. Work relevant for potential future Trials is described in section “Trial independent Test-bed integration”, which relates to internal solutions that were not selected for any of the 4 Trials, and in section “Considerations for future test and integration activities”. Annex 1 lists the DRIVER+ terminology, Annexes 2, 3 and 4 contain technical details (such as detailed data exchange diagrams, deployment diagrams, recorded UML sequence diagrams, etc.) for Trials 3 and 4 and for the Final Demo. Annex 5 provides detailed test reports for those internal solutions that were not selected for any of the Trials.

For a detailed description of each of the solutions, we refer the DRIVER+ Portfolio of Solutions: <https://pos.driver-project.eu/>

## 2. Solution integration process through the Test-bed

### 2.1 Solution integration process

Figure 2.1 gives a high-level overview of the DRIVER+ solution integration process. A more comprehensive description can be found in **D934.21 Solution Testing Procedure** (6).

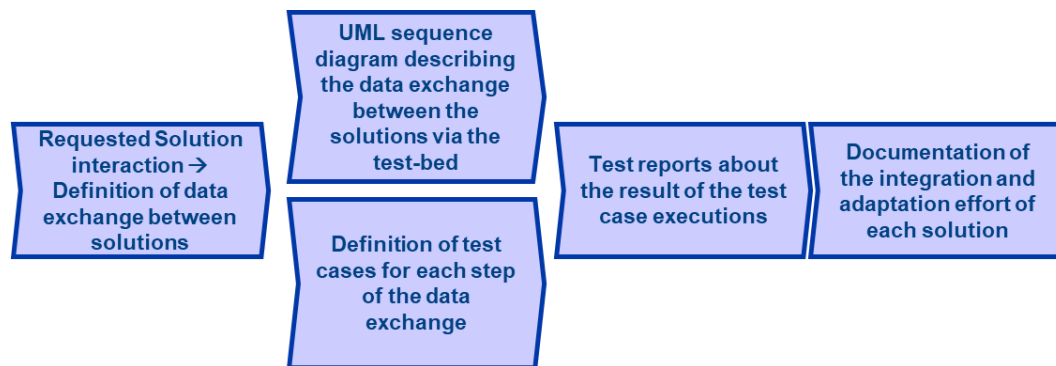


Figure 2.1: DRIVER+ solution integration process

On a generic level, the solution integration process consists of the steps listed below.

#### Identification of solution interaction

The process starts with the identification of the interaction requirements for each solution that shall be integrated. This includes an analysis of which data are expected to be received by a solution as input data and which data are expected to be provided by a solution as output data. For solutions taking part in a DRIVER+ Trial, this step leads to a high-level solution interaction description.

#### Detailed description of data exchange via Test-bed

Once the principle interaction needs of the solutions are known, a detailed data exchange analysis has to be performed, including the use of the Test-bed for the various data-flows. This analysis leads to the documentation of the data exchange in form of a detailed solution interaction diagram and UML sequence diagrams. For solutions taking part at a DRIVER+ Trial, the detailed data exchange sequences can be elaborated from the use cases being defined in the Trial scenarios. For solutions that are not selected for a Trial, specific use cases have to be defined for the integration, also assuming at least one “related solution” for data exchange (for example: data provided by solution X shall be visible in COP solution Y).

At technical level, in this phase the data structures have to be defined in detail, the appropriate Test-bed adapters have to be selected, communication channels have to be configured in the Test-bed infrastructure, solutions have to be adapted and modified accordingly in their front-ends and back-ends.

#### Definition of test cases

Parallel to the detailed definition of the data exchange, test cases have to be elaborated, aiming at verifying each step of the data exchange. For solutions taking part at DRIVER+ Trials, a subset of the Trial test cases may be used to verify the solution integration and its collaboration with other solutions. For solutions that are not selected for a Trial, specific test cases have to be defined corresponding to the use cases (for example: verify that solution X data are correctly converted and transferred to solution Y).

At the end of this phase, test cases are executed, either in the scope of a Trial (for selected solutions), or in a dedicated integration session (for non-selected solutions).

### Reporting the results of test execution

For each test case the result of the execution has to be reported. For solutions taking part at a DRIVER+ Trial, this report consists of an indication on the test run, where the test was successfully executed (Dry Run 1, Dry Run 2, Trial). For non-selected solutions, an explicit test report has to be written.

### Documentation of adaptation and integration work per solution

The activities in terms of configuration, integration work, software updates etc. needed for integrating a solution has to be finally documented.

## 2.2 Solution integration events

---

The organisation of each Trial in the DRIVER+ context included the following events:

- **Technical Integration Meeting (TIM):**  
The TIM is mainly dedicated to the definition of data exchange between participating solutions. As such, the main outcome of the TIM is conceptual work, leading to a detailed specification of interfaces, messages and interaction sequences.
- **Dry Run 1:**  
During Dry Run 1, the technical execution of the Trial is tried to be conducted for the first time in its entirety. This means, all participating solutions are tried to be integrated and all test cases are executed in order to evaluate the integration status.
- **Dry Run 2:**  
The Dry Run 2 is a kind of "dress rehearsal" for the Trial itself. This means, all participating solutions are expected to be integrated, all test cases are executed in front of end users. At this stage the integration work should be more or less finalised.
- **Trial execution itself:**  
This is the official execution of the Trial.

The solution integration steps have been defined in deliverable **D934.21 Solution Testing Procedure** (6). The goal of this procedure is to make sure that the solutions and the technical set-up are ready at the end of Dry Run 1 to support the Trial execution.

## 2.3 Brief description of the Test-bed

---

The Test-bed is an important part of the DRIVER+ project and is therefore dealt within its own sub-project, namely **SP92 Test-bed**. In the document at hand, only a brief overview is given of the Test-bed, its purpose and its design as there are several dedicated Test-bed deliverables (7), (8) and (9).

In DRIVER+ the Test-bed provides the necessary infrastructure to prepare, execute and manage Trials and in this context, evaluate the solutions which participate in those Trials. It is designed following a modular approach in the sense that several tools and services fulfilling a certain purpose each are connected to build-up the Test-bed. In this way, the Test-bed has been progressively extended during the course of DRIVER+. Also, the modular design should make the task of sustaining the Test-bed beyond the project's lifetime an easier one. As one of the Test-bed's main purposes is providing the infrastructure for connected systems to exchange information, the architecture of the Test-bed is message-based using the open-source messaging system Apache Kafka. Further, the Test-bed is intended to be deployed using composed Docker images, i.e. ready-to-use installer applications that facilitate an easy deployment, see <https://github.com/DRIVER-EU/>.



The next paragraph gives an overview the components of the Test-bed. A more detailed description of the Test-bed can be found in **D923.11** regarding the **Test-bed specification** (7) and in **D923.21** (8) and **D923.22** (9), which describes the design of the **Test-bed reference implementation**.

### 2.3.1 Test-bed components

The Test-bed consists of several modular tools and services. During the course of DRIVER+ the reference implementation of the Test-bed was constantly improved. Therefore, several versions were released. As a consequence, not all of the components described here were part of each Trial. For each Trial, the used Test-bed components are listed in the corresponding result section.

Figure 2.2 provides an overview of the architecture of the Test-bed and its components. The main components are specified in Table 2.1.

In addition to the components there are adapters specified and implemented in the reference implementation. Those adapters serve the purpose of data transfer, i.e. message exchange between the solutions and the Common Information Space (CIS adapters) and the simulations and the Common Simulation Space (CSS adapters), respectively. These adapters are also shown in Figure 2.2. Several types of adapters are currently available to provide easy integration of solutions and Simulators. Those include a REST<sup>1</sup> adapter, a TypeScript<sup>2</sup> adapter, a Python adapter, a Java adapter and a C# adapter.

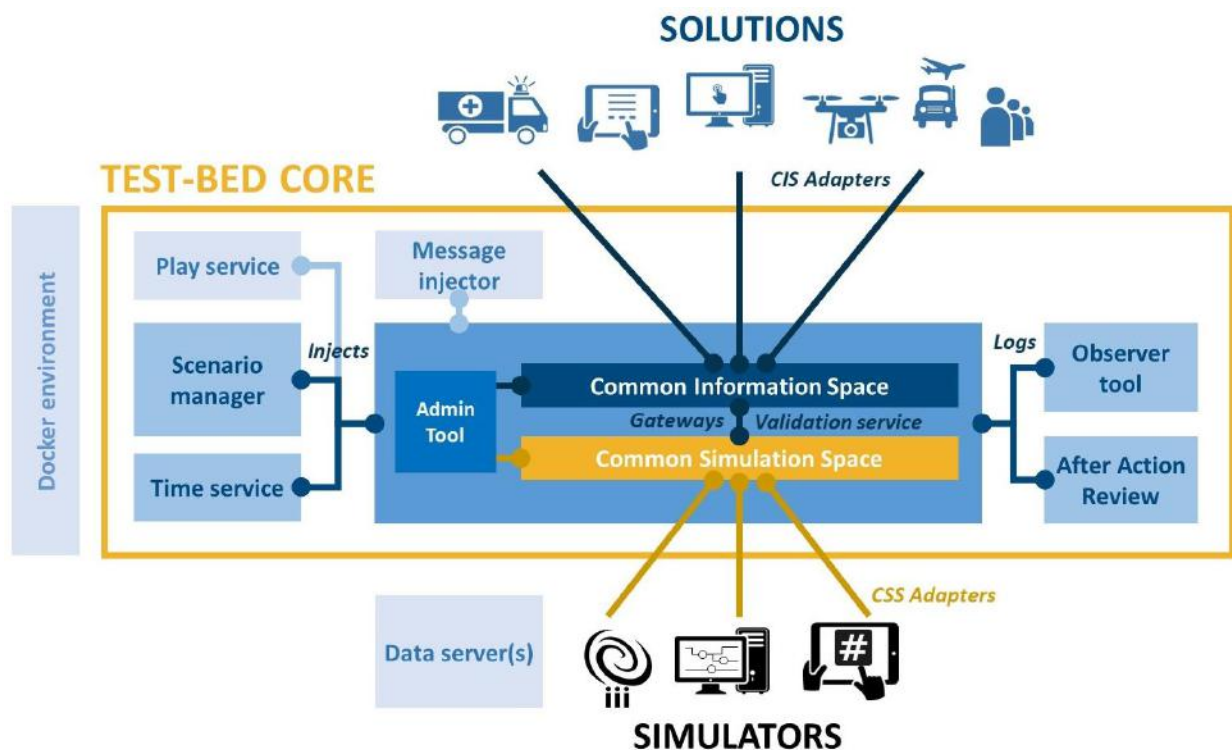


Figure 2.2: The Test-bed and its components

<sup>1</sup> Representational State Transfer (REST) is a web service for sharing information.

<sup>2</sup> TypeScript is an open-source programming language developed and maintained by Microsoft. It is a strict syntactical superset of JavaScript.

**Table 2.1: Main components of the Test-bed**

Component	Short description	Responsible
<b>Common Information Space (CIS)</b>	A central messaging bus facilitating interconnection between solutions.	FRQ
<b>CIS adapter</b>	Standardised SW component to connect solutions to the Test-bed.	FRQ
<b>Common Simulation Space (CSS)</b>	A central messaging bus facilitating interconnection between simulators.	TNO, XVR
<b>CSS adapter</b>	Standardised SW component to connect simulators to the Test-bed.	TNO, XVR
<b>Gateways</b>	Links between the CSS and the CIS to feed solutions with data from the Simulations and vice versa.	TNO
<b>Validation service</b>	A service that validates the messages sent between CSS and CIS. (optional)	TNO
<b>Test-bed Admin Tool</b>	A tool providing a user interface to control the CSS and CIS before and during a Trial.	FRQ
<b>Trial scenario manager</b>	A tool to create and manage the timeline of a Trial scenario. Also, messages might be prepared before the Trial and injected during Trial execution.	TNO
<b>Time Service</b>	A service that controls the fictitious time during a Trial.	TNO
<b>Observer Support Tool (OST)</b>	With the OST observations can be gathered during a Trial.	TNO, ITTI
<b>After Action Review (AAR)</b>	The AAR module uses data-logs and observations to review the Trial after it was executed.	FRQ

## 2.4 Solution integration information and support

The steps of the solution provider to integrate their solutions into the Test-bed are:

- Understanding the Test-bed concept.
- Understanding the Test-bed adapter options and choosing the right adapter for their solution.
- Defining the messages to be exchanged between the solution and the Test-bed.
- Connecting the adapter to their solution.
- Exchanging messages between solution and Test-bed.

To support this process, an integration information package was created in 2018 and has been updated several times in 2019 and made available under the following link: <https://github.com/DRIVER-EU/Test-bed#integration-process>.

With this information, solution providers could start their Test-bed integration with a local version of the Test-bed and try to connect their solution to one of the available Test-bed adapters.

As all technical support questions and answers related to Test-bed integration were assumed to be of interest for all solution providers, a communication channel was established in 2018 (and is still available)

in form of an online forum with the online communication tool SLACK under the following link:  
<https://driver-eu.slack.com/messages/C6YQK3FUJ/>.

### 3. Trial 3

This section describes the main activities related to the integration of solutions for Trial 3. Trial 3 mainly focused on volunteer management and aerial situation assessment in an earthquake scenario including heavy rain and landslides. The Trial also included a non-technical solution, the psychological first aid solution by DRC.

The Trial was organized by Austrian Red Cross (ÖRK) in combination with Austrian Institute of Technology (AIT) and was conducted in Eisenerz, Styria.

The main challenge of Trial 3 was that the Trial was executed in cooperation with a large-scale European disaster response exercise EUCP-EX (IRONORE2019) of the Austrian Red Cross with several hundred active participants<sup>3</sup>.

Before the execution of Trial 3 there was a Technical Integration Meeting and two Dry Runs (named DR1 and DR2) for the preparation of all technical and organizational matters. Table 3.1 lists the dates and locations for the different steps of Trial 3.

**Table 3.1: Dates and locations of TIM, DR1, DR2 and Trial 3 execution**

Event	Duration	Date	Location
TIM	3 days	11-13/03/2019	Eisenerz, Austria
Dry Run 1	5 days	13-17/05/2019	Eisenerz, Austria
Dry Run 2	5 days	19-23/08/2019	Eisenerz, Austria
Trial	4 days	12-15/09/2019	Eisenerz, Austria

#### 3.1 CM gaps covered in Trial 3

According to DRIVER+ methodology, the corresponding gap analysis was carried out for Trial 3. This analysis was intended to reveal areas that can be improved in the existing practices, processes and daily operations related to Crisis Management in the context described by the Trial scenario.

The gap analysis was conducted by the Trial Owner (Austrian Red Cross) in collaboration with their practitioners' network. The resulting list of gaps was presented during the DRIVER+ Gap Assessment Workshop where multiple stakeholders and practitioners were invited to discuss and assess the relevance of the presented gaps for them. After the received feedback, it was decided to focus with highest priority on the following gaps listed in Table 3.2.

**Table 3.2: Crisis Management high priority gaps covered in Trial 3**

Name	Gap description
Real-time data and information fusion to	Limits in the ability to merge and synthesise disparate data sources and models in real time (visualisation of resources spreading models, tactical situation,

<sup>3</sup> This is the reason why Trial 3 was performed after Trial 4.

Name	Gap description
support incident commander decision-making	critical assets map, etc.) to support incident commander decision making.
Volunteer Management	Insufficiencies in the management of spontaneous and affiliated volunteers on the crisis scene in terms of location, tasking, capabilities, and shift duration.

These CM gaps drove the solution selection process, which aimed to select the solutions best suited to close the gaps. The selection process for these gaps and the current capabilities of the legacy systems of the end-users involved in Trial 3 are described in **D945.11 Report on Trial Action Plan - Trial 3** (10).

### 3.2 Scenario description of Trial 3

*The central area of Austria has been struck by a heavy earthquake and subsequent heavy rains. The local region of Eisenerz (in Styria, Austria) is one of the most affected with missing persons, casualties, collapsed buildings, blocked roads, and endangered industries working with hazardous substances. Inhabitants have left their houses being afraid of aftershocks and collapsing of buildings. They must spend the next days outdoor due to the lack of temporary shelter and blocked roads. Similarly, there is a disruption of lifelines such as water, food, shelter, transportation and medical care. Electricity and mobile networks are severely damaged.*

*All local and national emergency response organizations have been deployed on site (Austrian Red Cross, fire brigades, police and the army); however, due to the extension of the affected area and overwhelmed national response capacities, the union civil protection mechanism was activated. A request of international assistance was activated with regards to medical treatment, water purification as well as search and rescue.*

*Due to the difficulty to access the affected area and considering the impact of the disaster, there is an urgent need for humanitarian assistance and assessment. A large amount of volunteers and rescue equipment is needed to deal with the increasing number of affected people i.e. search and rescue, shelter, medical care, water, food, and transportation. Additionally, there is also an urgent need for the management of spontaneous volunteers.*

The above scenario has been organised in 5 sub-scenarios, as listed below. Each sub-scenario is defined by a pre-planned storyline that drives an exercise, as well as by events used as stimuli for the individual solutions involved in the sub-scenario.

- **Sub-scenario #1: Emergent Groups (Telegram):**  
A large number of spontaneous volunteers (SV) which were self-organised on social media (Telegram) have started to build common kitchens and cleaning some areas for placing tents. A Media Team has identified this and has prepared the information to be shared with the Incident command which decides to send a small team to assess the situation and try to coordinate better the response.
- **Sub-scenario #2: Situation Assessment:**  
The incident command has been informed that the Local Region of Eisenerz is one of the most affected. Reports from the local Fire brigade inform about collapsed buildings and damages to critical infrastructure such as roads, pipelines, electricity and mobile Networks.  
Due to the limited number of first responders on site, the information of damages and the extent is unclear. The Incident Command requests an initial aerial assessment for identifying affected areas.
- **Sub-scenario #3: Confirmation:**  
The images from aerial assessment show some collapsed buildings, blocked roads and other facilities with a damage which is better visualised on vieWTerra Evolution. However, onsite images are needed

to confirm the level of damage. First responder units are far away from the areas and may take some time for them to reach the identified places. Incident Command decides to task onsite pre-registered volunteers to gather information from the area.

- **Sub-scenario #4a: Chemical Spill:**  
The local fire brigade has reported damages to a factory working with hazardous substances. Citizens report headaches and dizziness. The fire brigade and the police are evacuating the surrounding area as preventive measure. A safety zone is virtually created in the surroundings of the factory, and increased within the main wind direction. Any other Team in transit through that zone will receive an alert informing they have entered a dangerous zone. An aerial assessment is needed to assess the population that may be exposed.
- **Sub-scenario #4b: Emergent Groups (PFA):**  
The Red Cross has prepared for dealing with SV by training its CM staff (professionals or trained volunteers) in relating and working with spontaneous volunteers. A part of them is receiving instructions in psychological first aid, and they are accompanied by a trained team leader who is experienced in the subject.
- **Sub-scenario #5: USAR Teams, Communication:**  
A USAR Team has reached one of the remote affected areas identified in the aerial assessment maps. Due to network coverage problems, they are facing problems for communicating with the Incident Command. The Teams are equipped with a handheld device that can be used to send on-site imagery and data via satellite. A 360° video camera and tracking data of response units can be used to record the performed activities so that an incident response evaluation can be done.

For more details about the scenario of Trial 3 please see **D945.11 Report on Trial Action Plan – Trial 3** (10).

### 3.3 Participating solutions

As summarised in Table 3.3, Trial 3 was expected to be conducted with the participation of 3 internal solutions and 2 external solutions. 1 Backup solution (external) was selected for the case that a selected solution would withdraw.

**Table 3.3: Selected solutions for Trial 3**

Solution name	Solution provider
GINA (external)	Gina Software s.r.o / Czech Republic
viewTerra Evolution (external)	VWORLD / France
CrowdTasker	AIT / Austria
PFA (PSS) – Psychological First Aid (Psychosocial support)	DRC / Denmark
Airborne and Terrestrial Situational Awareness	DLR / Germany
<b>BACKUP SOLUTION:</b>	
ASIGN (external)	AnsuR / Norway

As GINA withdrew their solution, the Backup solution ASIGN took over this role. The functionality offered by ASIGN could replace the GINA functionality to a large extent.

Table 3.4 provides an overview of the solutions, including their role in Trial 3 and including references to their descriptions in the Portfolio of Solutions.

**Table 3.4: Solutions overview for Trial 3**

Solution	Short description
GINA <a href="https://pos.driver-project.eu/en/PoS/solutions/75">https://pos.driver-project.eu/en/PoS/solutions/75</a>	GINA System is a map software technology for computers, tablets and smartphones.  The GINA solution was withdrawn from Trial 3 and replaced by ASIGN solution.
viewTerra Evolution <a href="https://pos.driver-project.eu/en/PoS/solutions/94">https://pos.driver-project.eu/en/PoS/solutions/94</a>	viewTerra Evolution is a 4D Earth Viewer as well as a data & assets integration and development platform allowing Civil responders to build a virtual 4D representation (3D synthetic environment + Time dimension) of a potential Crisis area to provide a Common Operational Picture.  In Trial 3, the viewTerra Evolution suite is used to provide a Common Operational Picture in sub-scenarios #2, #3, #4a, #5.
CrowdTasker <a href="https://pos.driver-project.eu/en/PoS/solutions/20">https://pos.driver-project.eu/en/PoS/solutions/20</a>	CrowdTasker supports Crisis Management by instructing large numbers of non-institutional volunteers with customizable tasks, contextual information, warnings and alerts, as well as to crowdsource information from them.  In Trial 3, CrowdTasker is used in sub-scenarios #1, #3 and #4a.
PFA (PSS) – Psychological First Aid (Psychosocial support) <a href="https://pos.driver-project.eu/en/PoS/solutions/61">https://pos.driver-project.eu/en/PoS/solutions/61</a>	Psychological first aid (PFA) is a method of helping people in distress so they feel calm and supported in coping with their challenges.  In Trial 3, Psychological First Aid is applied in sub-scenario #4b.
Airborne and Terrestrial Situational Awareness <a href="https://pos.driver-project.eu/en/PoS/solutions/24">https://pos.driver-project.eu/en/PoS/solutions/24</a>	The “Airborne and Terrestrial Situational Awareness” solution is composed of several components, including an optical 3K camera system integrated into a research aircraft operated as a remotely piloted vehicle (RPV) during the Trial.  In Trial 3, DLRs Airborne and terrestrial situation awareness solution is used in sub-scenario #2.
ASIGN <a href="https://pos.driver-project.eu/en/PoS/solutions/99">https://pos.driver-project.eu/en/PoS/solutions/99</a>	ASIGN is an all-in-one disaster assessment software tool for the collection, communication and management of operationally relevant information.  In Trial 3, ASIGN is used in sub-scenarios #4a and #5.

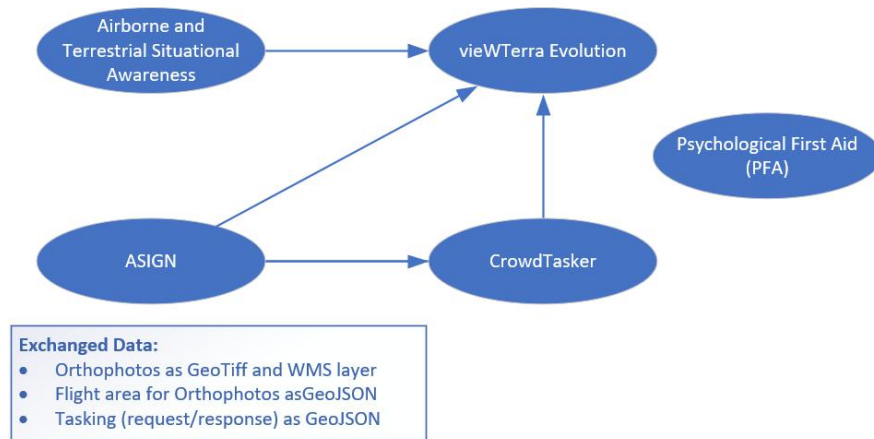
### 3.4 Trial 3 intended solution interaction

This section gives a high-level overview of the intended collaboration of solutions participating in Trial 3. Based on aerial images and additional data gathered by the Airborne and Terrestrial Situational Awareness solution, information layers relevant for Crisis Management shall be created. viewTerra Evolution allows rapidly building a virtual 4D representation (3D synthetic environment + Time dimension) of a crisis area and as such providing a Common Operational Picture to both the Crisis Centre and the rescue units out in the field. ASIGN shall enable field users to provide reports, marking geographical zones as dangerous areas



and share them with the Centre. CrowdTasker shall be used to coordinate teams and exchange information effectively. Finally, Psychological First Aid provides Guidelines on caring for staff and volunteers during and after crises.

Driver Solution Interaction - Trial 3 (Austria)



**Figure 3.1: Trial 3 solution interactions**

Figure 3.1 provides an overview of the intended communication channels between involved solutions in Trial 3. Each of the shown channels is realised via the messaging system provided by the Test-bed. The PFA appears as an isolated node in this figure, since it is not a technical solution like the others and therefore does not use the Test-bed for information exchange.

Table 3.5 provides an overview about how the individual solutions are integrated with the Test-bed on the technical level (which adapter to be used).

**Table 3.5: Trial 3 solution integration with Test-bed**

Solution	Test-bed adapter
Airborne and Terrestrial Situational Awareness	REST adapter
CrowdTasker	typescript/node.js adapter
viewTerra Evolution	REST adapter
ASIGN	Python adapter
PFA	- (*)

(\*) Psychological First Aid (PFA) is not a technical solution and does not use the Test-bed for information exchange.

More details of the finally realized solution integration and communication channels can be found in the sections below.

### 3.5 Trial preparation and execution

#### 3.5.1 Overview

The main focus of Dry Run 1 (DR1) was to perform initial tests and verify the technical integration of solutions and to document the results.

For DR2, the scenario for Trial 3 has been worked out in more detail; during DR2 the tests have been re-executed and some previously non-successful scenarios could be verified.

Dry Run 2 was also focusing on practitioners to learn the solutions' capabilities in the solution trainings.

From the technical perspective the overall objectives of Dry Run 2 were:

- Solution maturity check, organisational and technical constraints analysis.
- Solutions final integration with Test-bed.
- Theoretical and practical training on use of the solutions for Trial 3 participants.
- Running a pilot Trial 3 with practitioners' contribution ("dress rehearsal").
- Final check of readiness for Trial 3.

Figure 3.2 shows the final version of the overall solution interaction diagram, which evolved during the integration process. It illustrates the information exchanged between involved solutions in Trial 3 by making use of the Test-bed technical infrastructure.

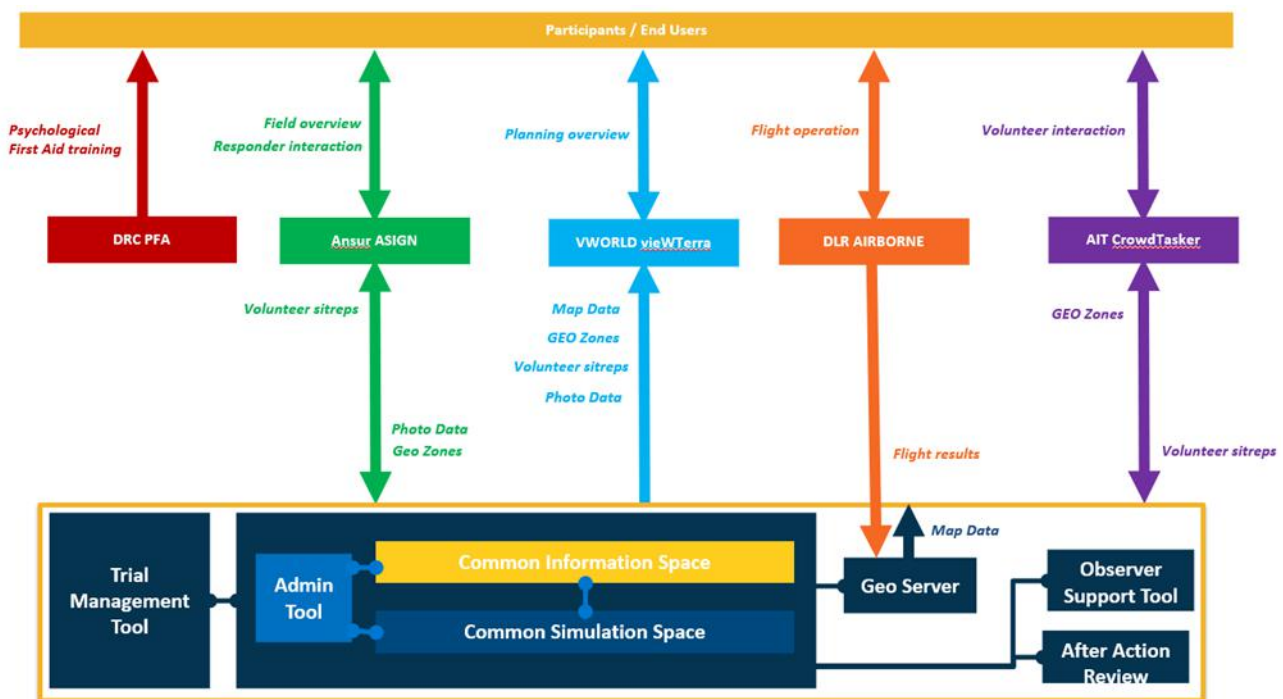


Figure 3.2: Solution interaction diagram for Trial 3

#### 3.5.2 Use cases

The use cases for Trial 3 have been elaborated on the basis of the sub-scenarios described in section 3.2 above. The information workflow between different solutions during each individual phase of the scenario has been analysed and is presented in this section. The elaborated use cases per sub-scenario are listed in

Table 3.6. A detailed description of each use case can be found in the Trial Action Plan (10). The table indicates a main target solution for each use case.

**Table 3.6: Use cases per sub-scenario in Trial 3**

Sub-scenario	Use case	Solution
<b>#1 Emergent groups - Telegram</b>	4 – Emergent groups	CrowdTasker
<b>#2 Situation assessment</b>	6 - Aerial assessment	Airborne
	8 - 3D operational picture navigation	viewTerra Evolution
<b>#3 Confirmation</b>	3 - Pre-registered volunteers	CrowdTasker
	7 - 2D overlay incident localization	viewTerra Evolution
	8 - 3D operational picture navigation	viewTerra Evolution
<b>#4a Chemical Spill</b>	2 - Hazardous zone notification	ASIGN
	8 - 3D operational picture navigation	viewTerra Evolution
<b>#4b Emergent Groups - PFA</b>	5 - PFA tasking	PFA
<b>#5 USAR Teams - Communication</b>	1 - No reception assessment	ASIGN
	8 - 3D operational picture navigation	viewTerra Evolution

The following sub-sections describe the use of solutions per sub-scenario. UML sequence diagrams are included for those sub-scenarios, where different solutions interact with each other, providing details about the interaction between solutions and the Test-bed.

### 3.5.2.1 Sub-scenario #1: “Emergent Groups – Telegram”

In sub-scenario #1, the Community component of CrowdTasker is used to organise the distribution of water/meals (or similar tasks). Emergent volunteer groups are supposed to address this problem autonomously. At the same time, CrowdTasker is used to organise specific tasks with individual spontaneous volunteers.

Since only the CrowdTasker solution was used during the “Emergent Groups - Telegram” sub-scenario, no inter-solution data exchange took place.

### 3.5.2.2 Sub-scenario #2: “Situation Assessment”

Figure 3.3 illustrates the inter-solution data exchange taking place during the Situation Assessment sub-scenario. After the Airborne solution has been used to create flight requests and to control the flight and taking pictures, the Airborne solution creates and stores imagery data. Airborne announces the availability of new data by distributing LargeDataUpdate indication messages to the Test-bed. As a result, the new data are downloaded to the GeoServer via FTP and converted to the WMS format. The GEO Server announces the existence of new data by sending a map\_update message to the Test-bed. The viewTerra Evolution solution is subscribed at the Test-bed to receive this kind of messages and gets therefore informed about the availability of new data at the GEO Server. As a result, viewTerra Evolution retrieves the imagery data from the GEO Server via WMS request.

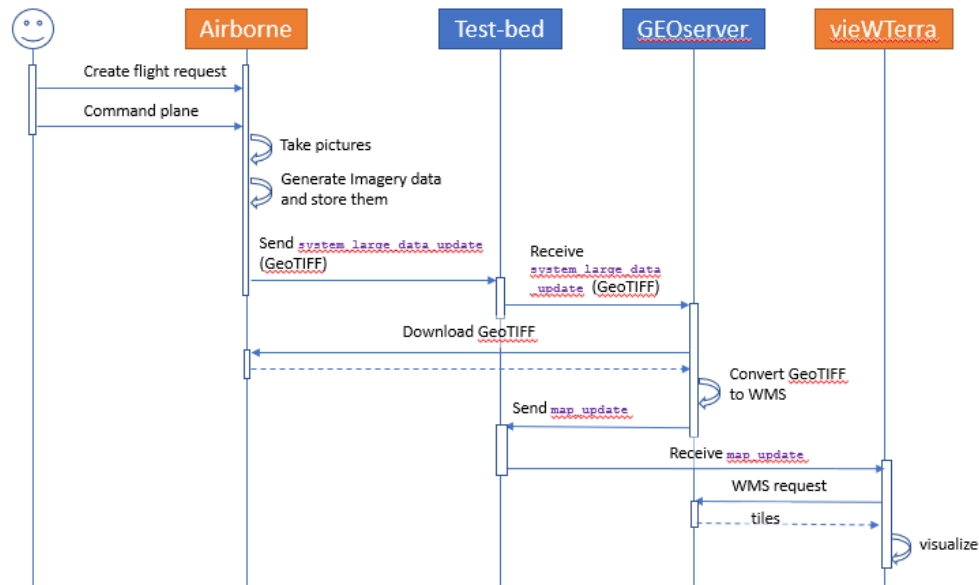


Figure 3.3: Interaction sequence diagram for the Situation Assessment phase (sub-scenario #2)

### 3.5.2.3 Sub-scenario #3: “Confirmation”

Figure 3.4 shows the inter-solution data exchange during the “Confirmation” sub-scenario. In this sub-scenario the CrowdTasker solution is used to define geographical zones and to distribute tasks to individuals. Individuals take pictures and provide them together with information to the CrowdTasker solution which announces the existence of new pictures to the Test-bed in a dedicated communication channel (topic “crowd\_tasker\_info”), encoded in the GeoJSON format. The vieWTerra Evolution solution is subscribed at the Test-bed to receive this kind of messages and is therefore informed about the availability of new pictures in the CrowdTasker solution. As a result, vieWTerra Evolution retrieves the pictures by downloading them directly from the CrowdTasker server.

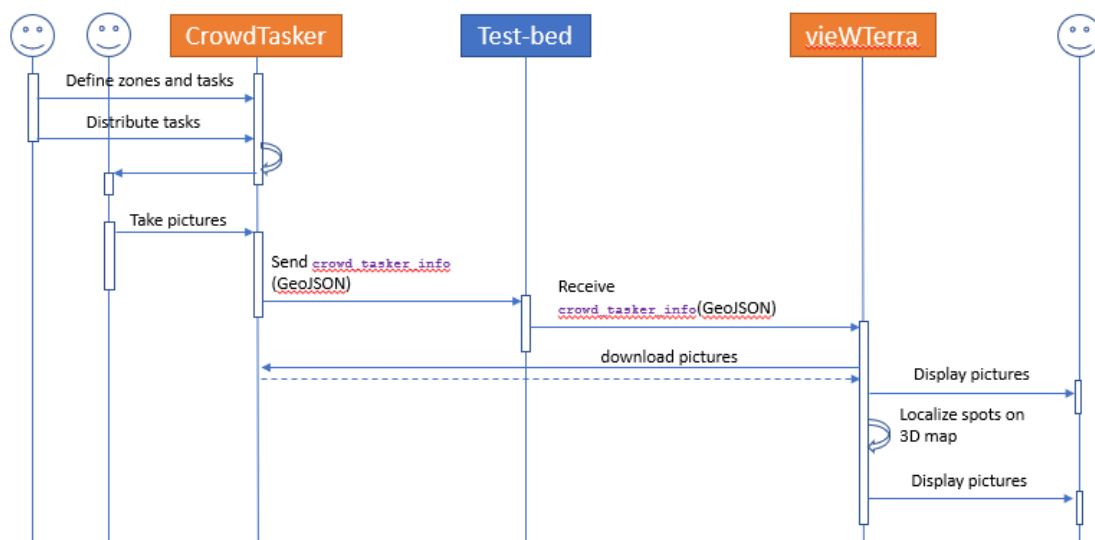


Figure 3.4: Interaction sequence diagram for the Confirmation phase (sub-scenario #3)

### 3.5.2.4 Sub-scenario #4a: “Chemical Spill”

Figure 3.5 gives an overview of inter-solution data exchange during the “Chemical Spill” sub-scenario. Operators of the ASIGN solution create report about the chemical spill and mark the affected geographical

area. ASIGN generates corresponding messages, describing the affected area in GeoJSON format and sends these messages to the Test-bed in a dedicated communication channel (topic “assign\_info”). Solutions viewTerra Evolution as well as CrowdTasker are subscribed at the Test-bed for this channel and therefore they both receive the GeoJSON messages provided by ASIGN.

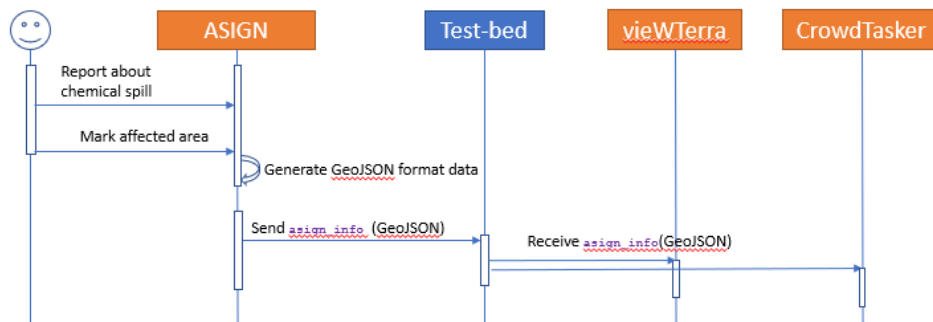


Figure 3.5: Interaction sequence diagram for sub-scenario #4a (Chemical spill)

### 3.5.2.5 Sub-scenario #4b: “Emergent Groups - PFA”

Since only the PFA solution was used during the “Emergent Groups - PFA” sub-scenario, no inter-solution data exchange took place.

### 3.5.2.6 Sub-scenario #5: “USAR Teams - Communication”

Figure 3.6 shows the inter-solution data exchange during the “Communication” sub-scenario. The data exchange in this sub-scenario is very similar to the one for the “Chemical Spill” sub-scenario. The difference is mainly in the gathering of data inside ASIGN solution, also using a satellite link (Satcom device) and in the format of the exchanged data; the data exchange steps are equivalent to the previous sub-scenario: ASIGN generates corresponding messages, describing reports (including pictures) in PhotoGeoJSON format and sends these messages to the Test-bed in the same communication channel (topic “assign\_info”). Solution viewTerra Evolution is subscribed at the Test-bed for this kind of messages and therefore receives the PhotoGeoJSON messages provided by ASIGN.

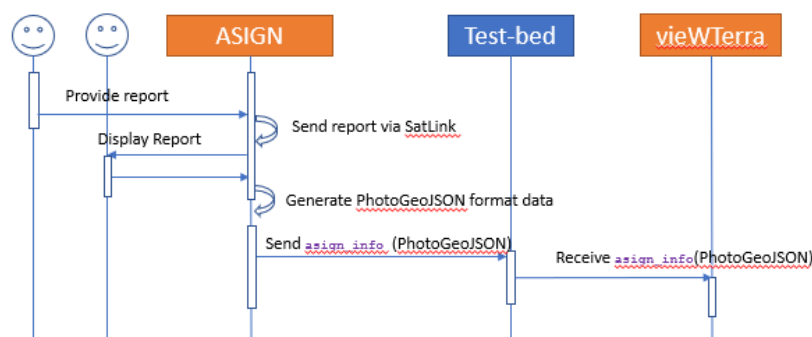


Figure 3.6: Interaction sequence diagram for Communication phase (sub-scenario #5)

## 3.5.3 Test cases

During DR1 and DR2 some 80 test cases were performed and evaluated. Most of these test cases are not relevant for solution integration, as they only involve operations performed at or with a single solution. Only a sub-set of the test cases involve two or more solutions, or a solution and the Test-bed. Table 3.7 lists this sub-set of test cases, as they are the ones to be investigated and evaluated with respect to solution integration.

**Table 3.7: Test cases related to solution integration performed in Trial 3 DR1 and DR2.**

Test-case	User	Using solution	Description	Receiving user	Via solution
1.5	Airborne operator	Airborne	Process and Publish Aerial images to Test-bed.	Test-bed	
1.6	Test-bed	Geo-server	Convert images and publish WMS service to Test-bed.	Test-bed	
1.7	Test-bed		Notify vieWTerra Evolution on update.	vieWTerra Evolution operator	vieWTerra Evolution
2.11	CrowdTasker operator	CrowdTasker	Publish answer report to Test-bed.	Test-bed	
2.12	CrowdTasker operator	CrowdTasker	Publish volunteer image to Test-bed.	Test-bed	
2.13	Test-bed		Import answer report.	vieWTerra Evolution operator	vieWTerra Evolution
2.14	Test-bed		Import image taken by a volunteer.	vieWTerra Evolution operator	vieWTerra Evolution
3.5	ASIGN operator	ASIGN	Publish the zone shape to the Test-bed.	Test-bed	
3.6	Test-bed		Import the zone shape from the Test-bed.	vieWTerra Evolution operator	vieWTerra Evolution
3.8	Test-bed		Import the zone shape from the Test-bed.	CrowdTasker operator	CrowdTasker
4.8	ASIGN operator	ASIGN	Publish received geo-images to Test-bed.	Test-bed	
4.9	Test-bed		Import geo-images from Test-bed.	vieWTerra Evolution operator	vieWTerra Evolution
4.13	ASIGN operator	ASIGN	Obtains detailed region of interest and automatically publish.	Test-bed	
4.14	Test-bed		Import geo-image magnification from Test-bed.	vieWTerra Evolution operator	vieWTerra Evolution

A technical data exchange diagram summarizing which kinds of data have been exchanged between which solutions in the scope of which test cases is provided in Figure A2.1 in Annex 2.

### 3.5.4 Solution integration results

Map centric solutions play a central role in the integration process as they are the medium of choice to display results from other solutions which can be geo-referenced. Using a map as the primary information layer opens the possibility to achieve a very structured presentation of information, with similar information types grouped in layers which can individually be switched on and off for best visibility of information.

The overall information flow diagram in Figure 3.7 shows the involved solutions and the information exchanged among them. Although they look similar, there is a difference in the meaning of the sequence diagrams here and in previous sections. While the diagrams shown in 3.5.2 were used to specify the integration needs during the elaboration phase, the figure here presents the final result.

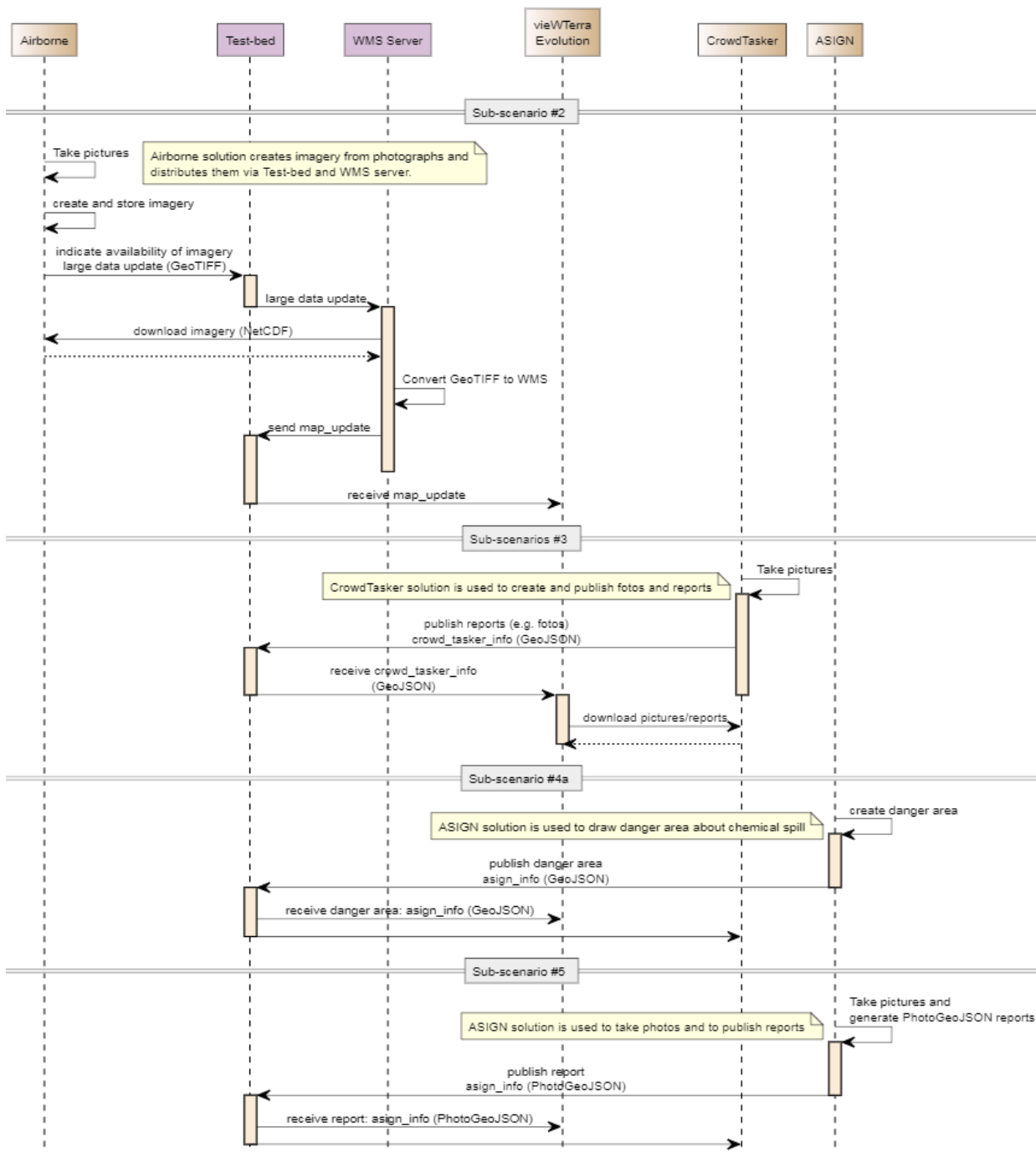


Figure 3.7: Overall information flow sequence diagram for Trial 3



### 3.5.4.1 Test-bed integration details

The Test-bed components used in Trial 3 were:

- The Test-bed itself.
- The Admin Tool.
- The Trial Management Tool (TMT).
- The Test-bed GeoServer.
- The Observer Support Tool (OST; online/offline mode).
- After-Action Review tool (AAR tool).

The Test-bed facilitates data exchange between solutions by so-called “topics”, which are pre-configured communication channels in the Test-bed, allowing broadcast/multicast communication (one solution sends data, many solutions may listen to these data) as well as point-to-point communication between dedicated solutions. On one hand, each solution may publish messages of a certain type onto certain topics; on the other hand, each solution may subscribe at certain topics in order to receive all messages that are published on that topic. More details on the topics used in Trial 3 can be found in Figure A2.3 in Annex 2.

### 3.5.4.2 Results of the test cases

The validation exercises related to solution integration consist of the consecutive execution of the test cases described in section 3.5.3.

Table 3.8 provides an overview of the test cases and test results achieved in DR1 and DR2. All test scenarios could be successfully tested either in DR1 or in DR2.

**Table 3.8: Test cases and test results achieved in DR1 and DR2**

Test Case	Title	DR1	DR2
1.5	Process and Publish Aerial images to Test-bed.	OK	OK
1.6	Convert images and publish WMS service to Test-bed.	OK	OK
1.7	Notify vieWTerra Evolution on update.	OK	OK
2.11	Publish answer report to Test-bed.	OK	OK
2.12	Publish volunteer image to Test-bed.	OK	OK
2.13	Import answer report.	OK	OK
2.14	Import image taken by a volunteer.	partly	OK
3.5	Publish the zone shape to the Test-bed.	OK	OK
3.6	Import the zone shape from the Test-bed.	OK	OK
3.8	Import the zone shape from the Test-bed.	OK	OK
4.8	Publish received geo-images to Test-bed.	OK	OK
4.9	Import geo-images from Test-bed.	partly	OK
4.13	Obtains detailed region of interest and automatically publish.	OK	OK
4.14	Import geo-image magnification from Test-bed.	OK	OK

The columns DR1 and DR2 indicate which test cases were successfully executed during Dry Run 1 and Dry Run 2, respectively. The table shows that some test cases were not fully successful during the first Dry Run, but all of them could be performed during the second Dry Run.

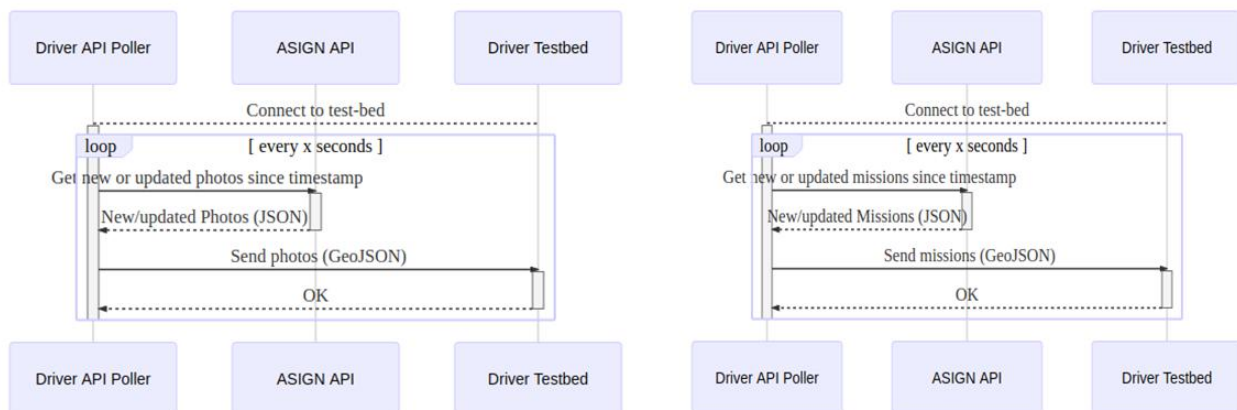
### 3.6 Solution providers' adaptations and integration technical details

This section contains descriptions of each solution provider regarding the adaptations which were needed in the solution to enable the support of the Trial 3. Necessary adaptations are described in terms of UI (User Interface) adaptations as well as back-end adaptations, i.e. changes that were made in controllers and the design of the Test-bed connection.

#### 3.6.1 ASIGN

This section describes the Test-bed integration for the ASIGN solution.

The ASIGN DRIVER+ integration was implemented as an adapter that polls resources from the ASIGN API and converts them to the corresponding DRIVER GeoJSON format before sending them to the DRIVER Test-bed. There are currently two ASIGN resources that can be exported to the DRIVER Test Bed: Geo-tagged Photos and Geo-located Missions.



**Figure 3.8: Sequence Diagram for the ASIGN to Test-bed Photo and Mission adapters**

The list below gives a summary of performed development work:

- Evaluate integration options and which adapter to use. The Python adapter was chosen.
- Install Test-bed locally and try sending/receiving messages from the Test-bed using the Python adapter.
- Create and test data schemas for ASIGN photos and missions with other solution providers.
  - For missions it was possible to reuse an existing standard GeoJSON schema.
  - Photos required a new complex schema definition and several iterations.
- Add a way to include Field of View information (used by viewTerra Evolution) for photos from a list of known camera models.
- Design, Implement and test Python-based solution that continuously gets updates from ASIGN, converts it to the required schema and pushes it to the Test-bed.
  - API Polling system supporting being started/stopped and continuing from last known timestamp.
  - Mission adapter converting from ASIGN API Mission JSON format to DRIVER Mission GeoJSON format.
  - Photo adapter converting from ASIGN API Mission JSON format to DRIVER Photo GeoJSON format.

- Create Docker deployment configuration for the photo and mission exporter and deploy it on an Amazon Server.
- Supported all test and Trials towards Test-bed, including starting/stopping API as requested by Test-bed technical team.

### 3.6.2 vieWTerra Evolution

This section provides an overview about VWORLD development and integration efforts for Trial 3.

#### Connection to Test-bed

The REST API adapter has been used for the Test-bed connection. The interface with the adapter was programmed in C/C++ language with the usage of the WinSock library. Specific C/C++ functions have been written for

- Sockets initialization & closing.
- Topics registration.
- Messages pooling & call-back.
- Error treatment (disconnection, buffer errors, socket errors).

#### Test-bed messages interfacing

- Writing functions to interface vieWTerra Evolution with messages received from the Test-bed.
- Parsing of JSON (& GeoJSON) messages and treatment of potential errors (e.g. unexpected empty messages received during DR1).
- According to information parsed, calling of various vieWTerra Evolution SDK functions in order to:
  - Add 3D pins & labels for CrowdTasker (CT), ASIGN & DLR assets.
  - Attach Test-bed messages to pins.
  - Add 2D windows for messages information display (sender ID, GPS location, content etc.).
  - Display danger area/mission zones (polygons, CT & ASIGN).
  - Display 2D geotagged photos (CT).
  - Display 2D geotagged & geo-oriented photos (ASIGN).
  - Add DLR WMS 2D Imagery streams in vieWTerra Evolution.
- Evolution Layers Tab and allow draping of these over the vieWTerra Evolution 3D terrain.

#### Development of specific features for the need of Trial 3

- Trace Window: allowing easy navigation by simple click on message name/info.
- On-the-fly messages Log System, avoiding any potential loss of information in case of system failure.
- Action-Replay System allowing replaying the messages recorded during a session.
- Adjustment system for ASIGN photos, allowing the operator to adjust the photos' GPS location, direction, FOV & transparency of each photo, including storing/saving of this edited information.
- Hide/unhide feature for each message, allowing the operator to potentially hide/unhide a message.

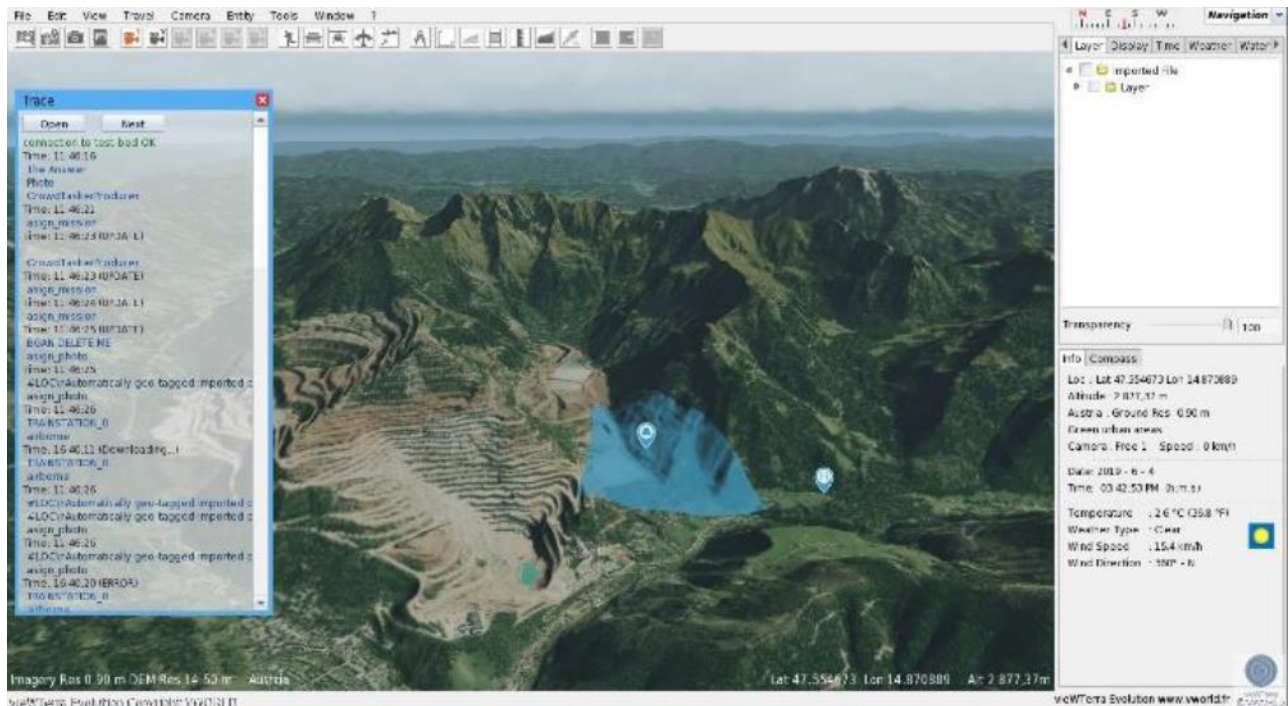


Figure 3.9: viewTerra Evolution example screenshot

#### Provision of specific databases

- Search for, treatment and integration of databases for the Eisenerz region:
  - DLR Imagery and Digital Surface Models (DSM) tests.
  - 3.6m RGB Copernicus Imagery (very High Resolution Image Mosaics) 2504 sq. km. Colour treatment and cloud removal.
  - 3.6m Copernicus Land Cover (ESM 2012 - 2017 release) 2504 sq. km colour classification correspondence.
  - 90cm RGB DigitalGlobe Imagery: 416 sq. km colour treatment and cloud removal.
  - 14.5m DTM (Open Data Österreich): 2965.6 sq. km.
  - Shapefiles creation (Open Street Map - roads, waterways & railways).
  - Footprints creation (Open Street Map).

#### Technical suggestions made by VWORLD and adopted for the Trial

- Definition of a colour code for cognitive interpretation of messages (DLR, CT & ASIGN).
- Integration of BBOX information into the JSON message sent through the Test-bed to inform of reception of a new WMS layer (map\_layer\_update) so as to allow minimizing the number of requests on the GeoServer and managing up to 25 different WMS layers for the integration of large DLR areas. This GeoServer optimization feature will be also proposed to be used for the upcoming Final Demo.

#### Testing sessions & adjustments

- In-house off-line tests.
- On-line testing using Test-bed TB6.

#### Telco meetings participations / TIM, DR1 & 2 and Trial participation

- Average of one 45min to 1-hour telco per week / Full participation from TIM to Trial.

### 3.6.3 CrowdTasker

This section provides an overview about the development and integration efforts for integrating the CrowdTasker solution into Trial 3.

### **Adaptations for connecting to and exchanging information with the Test-bed:**

- Implementation of specific message formats for the Trial:
  - GeoJSON for receiving AnsuR alerts.
  - GeoJSON for forwarding task and observation reports to viewWTerra Evolution.
  - GeoJSON for sending reports about message board activity of emergent groups to the Test-bed.
- Test-bed data visualization: extensions of the administrative frontend to support display of Trial specific message formats.
- CrowdTasker reports for the Test-bed: adding graphical user interface components and business logic to provide reporting functionality for sharing information on the Test-bed.
- Logging: messages going to, or coming from, the Test-bed, are logged for debugging and error handling purposes.
- Test-bed connection controls: extensions to the administrative frontend to allow for manual opening and closing of the connection to the Test-bed.

### **Adaptions and improvements of features specifically for the Trial:**

- Extending the user interface, business logic and data persistence layer to allow feedbacks and reports to be deleted.
- Extending the user interface, business logic and data persistence layer to allow deleting messages sent by other solutions in the Trial.
- Extending the user interface of interactive maps to support the display of latitude and longitude as well as an option to directly set coordinates for visualization.
- Adapting the iOS Version of CrowdTasker; to match the status of the Android CrowdTasker application (necessary due to the diverse device range of participants).
- Enhancing CrowdTasker task view on mobile applications by including a map component (participant requirement).
- Improving reliability of the CrowdTasker mobile application (both Android and iOS):
  - Local storage of messages in case of bad/no connection.
  - View for showing the status of the message (sent/pending).
  - Periodic polling, i.e. heartbeat, to check online status of the server.
- Adapting the social media module's data structure and interaction design to support more generic topics.
- Integrating the Telegram social media module with the CrowdTasker core platform to provide a more unified frontend in CrowdTasker.

### **Configuration and Trial Setup:**

- Configuration and deployment of a server instance for use in the Trial.
- Adaptation of the CrowdTasker application configuration (server side) to correspond with the Test-bed connectivity requirements (e.g., ports and URIs).
- Configuration of the continuous integration and deployment procedures of CrowdTasker to accommodate deployment and use in the Trial.

### **General Efforts:**

- Participation in weekly teleconferences for Trial and Dry Run preparations as well as coordination and communication efforts with other participating solutions.
- Increased testing efforts for CrowdTasker functionality due to added complexity of the Test-bed connection.
- Testing integration with other solutions to establish syntactical and semantic interoperability.
- Participation in meetings and events (TIM, DR1, DR2, Trial).



### 3.6.4 Airborne and Terrestrial Situational Awareness

The integration, adaptation and test effort for the Airborne and Terrestrial Situational Awareness solutions for Trial 3 was as described in this section.

#### Connectivity and Test-bed

- REST adapter of Test-bed implemented in U-Fly.
- Reception of GeoJSON messages in U-Fly (unused in Trial).
- Observation of folder on FTP server.
- Sending of LargeDataUpdate messages when a new image mosaic is available.
- Internal communication based on airborne data links (which were already available), WiFi and FTP services.

#### Development of specific features for Trial 3

- Mission planning module in U-Fly received terrain collision hints for the operator.
- Ground planning module was set to reduced performance for safety reasons.
- Multiple flight plans for mountainous regions developed and discussed with experimental pilots.
- Verification of the flight plans in the DLR simulation environment.
- New holding pattern implemented.
- Development of the interface from image processing server to U-Fly (DLR internal).
- Preparation and provision of an FTP server.
- Adjustment of the sending and receiving image processes due to specific configuration of the Trial (relay link mountain/ground).
- Adaptation of image products/interfaces for VWORLD:
  - Re-projection of mosaics to geographical coordinate system.
  - Adjustment of mosaic size to 10.000x10.000 pixels.
  - Categorization of mosaics according to the different scenarios.

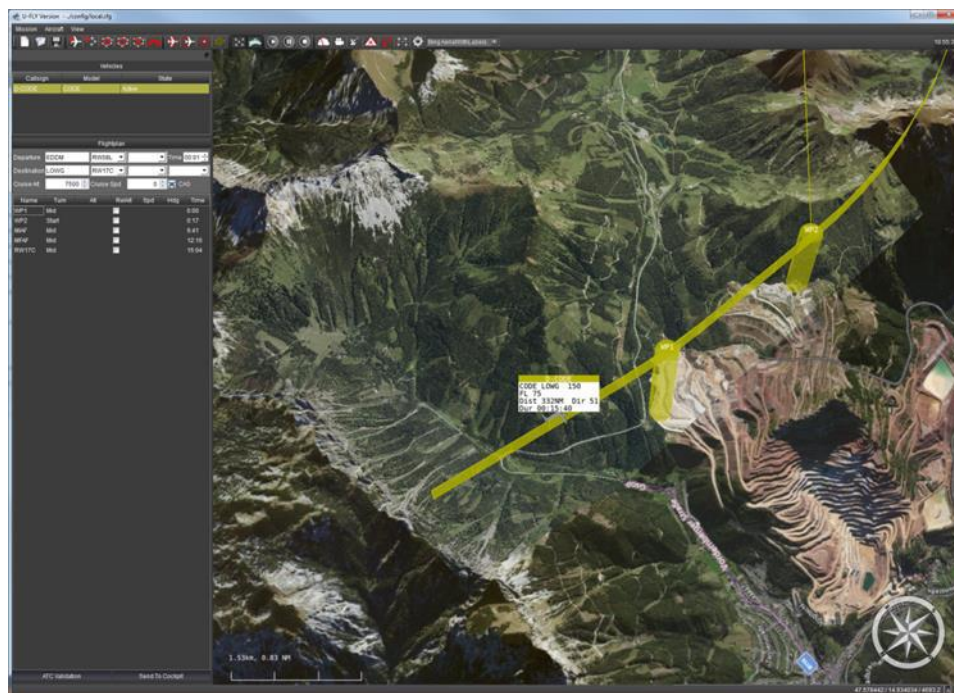


Figure 3.10: Mission planning capabilities in U-Fly

#### Technical adaptation of sensors/aircraft and flight permissions

- Intensive aircraft integration activities.

- Procurement of radio permission.
- Adapting the airworthiness certificate for the 3K camera system.
- Adjusting the sensor configuration and calibration.
- Adjusting the data link to mountainous regions.

#### **Preparatory testing sessions**

- In-house offline tests via ftp server and test data.
- In-house offline tests with ground station and data link to the airplane.
- Integration week (including flights) before Trial.

#### **Preparation of reference and test image data before Trial**

- Procuring reference data from the land of Styria.
- Preparing data from the land of Styria according to the requirements from VWORLD.
- Provision of test and reference data on an FTP server.
- Acquiring and processing data from Eisenerz (20 cm resolution) in the week before the Trial.
- Computing a digital surface model (DSM) and mosaics from the city of Eisenerz.
- Providing the DSM and the mosaics to the Centre for Satellite based Crisis Information (ZKI) for the generation of map products.

#### **Preparation and adaptation of map products**

- Update of concept and template design due to user feedback received.
- Data research and procurement (elevation, raster, vector data).
- Preparation of map drafts for DR2.
- Provision of additional data and AOIs on request.
- Update of map extents on request.
- Preparation of final map products as reference maps and map updates based on new data acquisition by DLR.

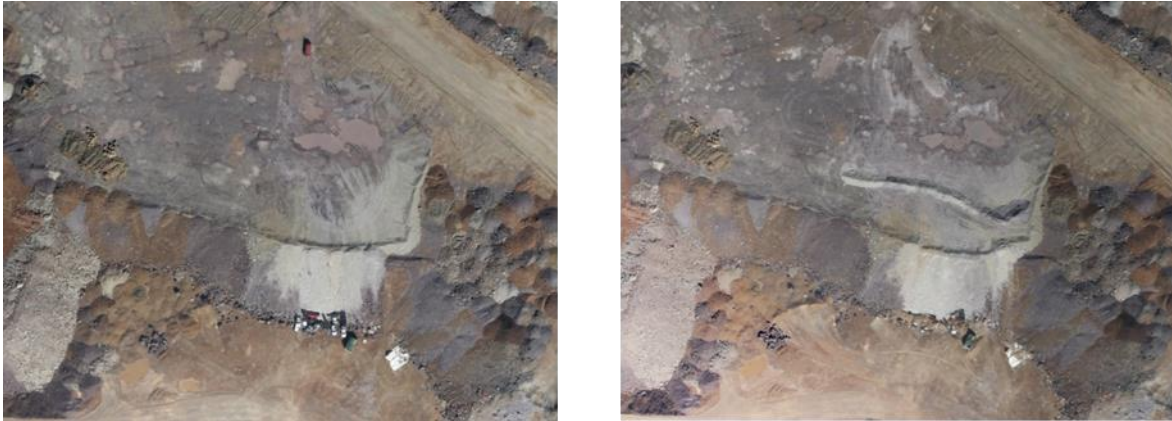


**Figure 3.11: Generated digital surface model (DSM)**

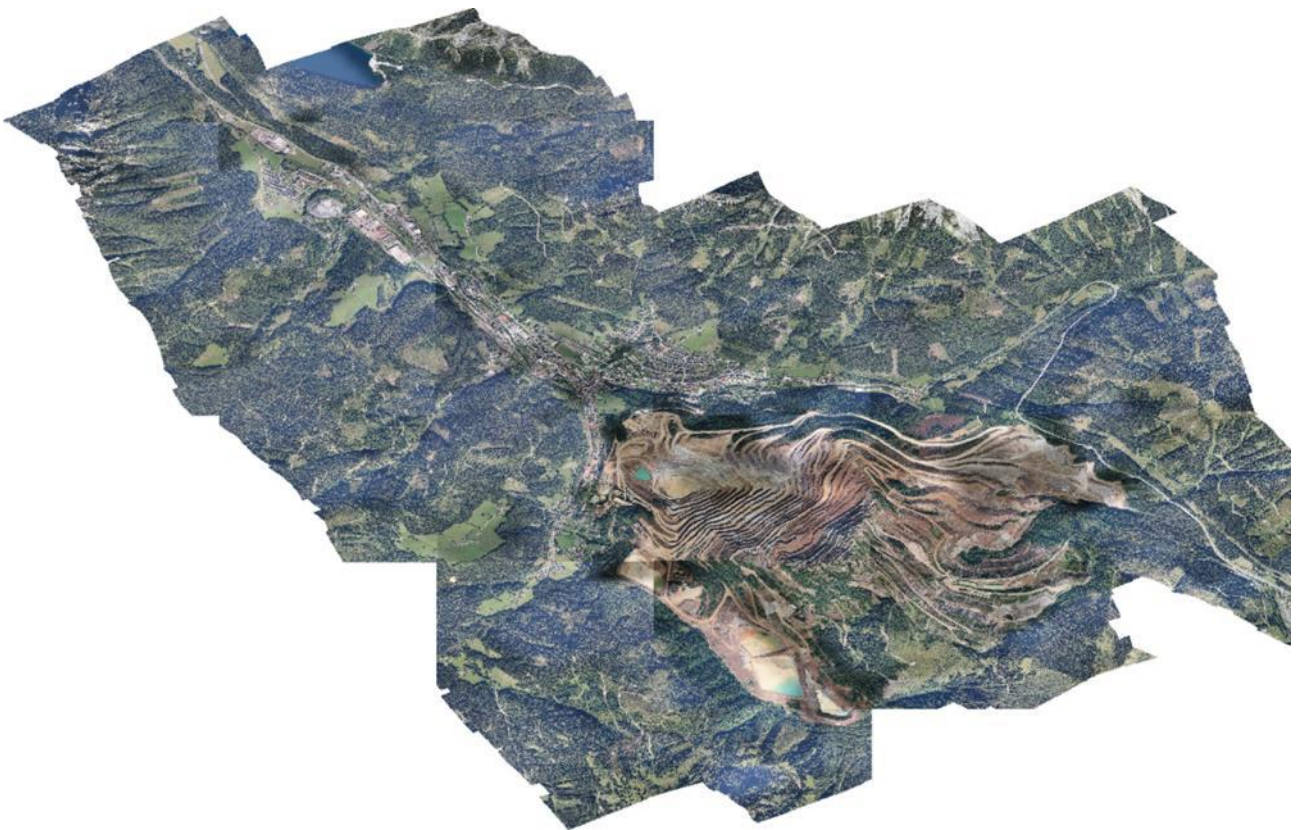
#### **Provision of image data and map products**

- Provision of 75 mosaics with a resolution of 15cm out of two flight days on FTP server.
- Provision of single images to U-Fly via FTP server.
- Provision of pre- and post-disaster image quick looks of simulated landslides in QGIS.
- Three 2D GeoPDF, five 3D PDF, one ArcGIS Pro Scene for DR2 (Drafts).
- Six 2D GeoPDF, five 3D PDF, one ArcGIS Pro Scene (Reference Maps).
- Four 2D GeoPDF, three 3D PDF, one ArcGIS Pro Scene (Map Update).
- Plots of 2D products.



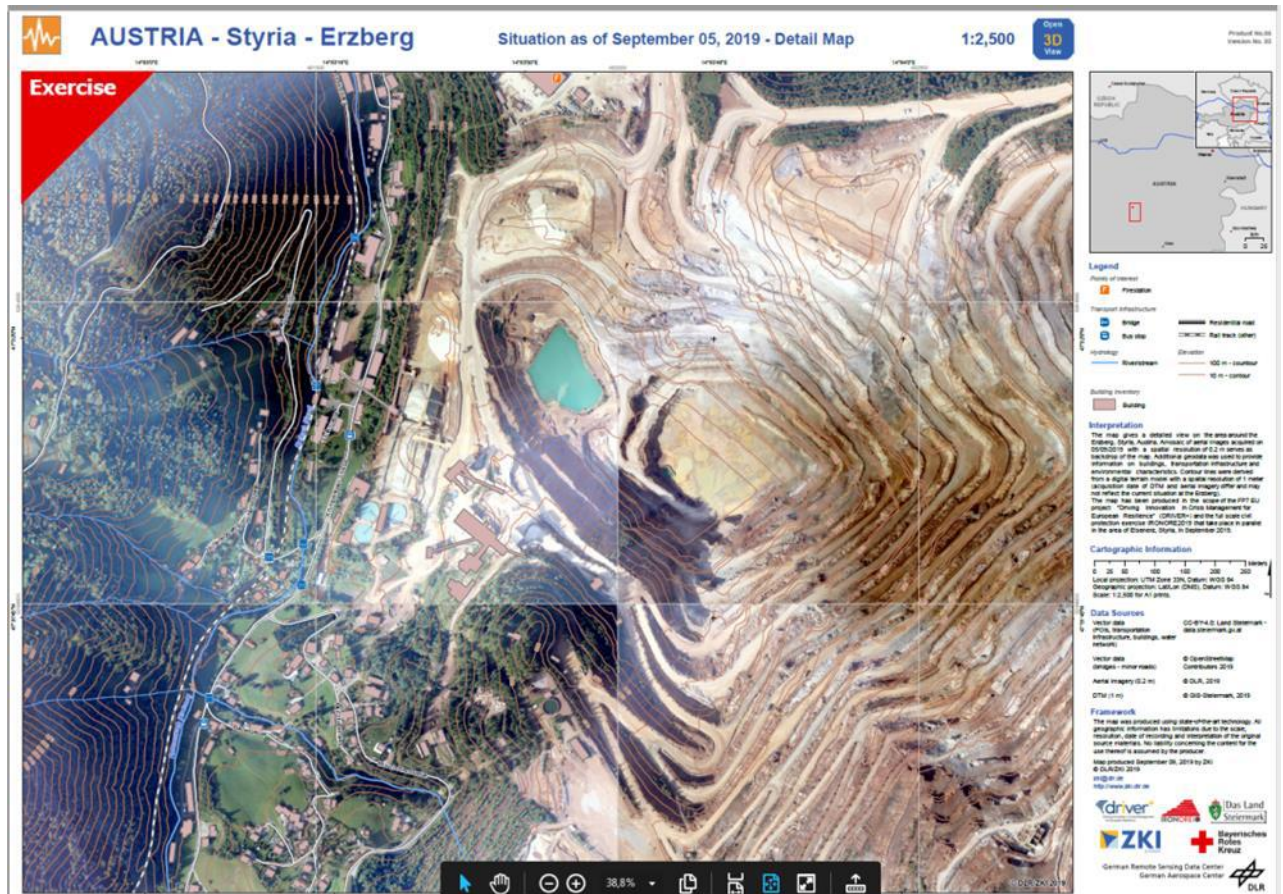


**Figure 3.12: Pre- and post-disaster landslide**



**Figure 3.13: Mosaic with 15 cm resolution**





**Figure 3.14: Plotted 2D map product**

## 4. Trial 4

This section describes the main activities related to the integration of solutions for Trial 4. The Trial was organized by Safety Region Haaglanden (SRH) and was conducted as a table-top Trial at the premises SRH (The Hague).

The main challenges of Trial 4 were:

- The amount of involved solutions was increased to 6 solutions.
- The involvement of a legacy solution (LCMS) which is in operational use for many years at several organisations in the Netherlands and which had to be prepared for data exchange with other involved solutions.
- Security related functionality was added to the Test-bed in Q1-2019 and was tested for the first time in Trial 4.

A special challenge was the fact that external solution providers had to make their solutions compliant to the security standards of the Test-bed (compared to Trial 1 and 2, where no security functionality was used).

Trial 4 had one preceding technical integration meeting (TIM) and two preceding Dry Runs (named DR1 and DR2) in order to prepare the Trial properly, both from a technical and an organizational perspective. The dates and locations the TIM, DR1, DR2 and the Trial are listed in Table 4.1.

**Table 4.1: Dates and locations of DR1, DR2 and Trial 4 execution**

Event	Duration	Date	Location
TIM	4 days	13-16/11/2018	The Hague
Dry Run 1	5 days	18-22/02/2019	The Hague
Dry Run 2	5 days	08-12/04/2019	The Hague
Trial	5 days	20-24/05/2019	The Hague

Trial 4 with a flooding scenario was mainly focusing on interworking of solutions to solve the challenges of this disaster. The Trial itself also served as a demonstration of the potential of how a legacy solution could be integrated with several new, innovative solutions.

### 4.1 CM gaps addressed in Trial 4

Table 4.2 lists the high priority gaps which were selected to be addressed by the solutions in Trial 4.

**Table 4.2: CM gaps addressed in Trial 4**

Name	Gap description
Planning of resources	Limitations in the planning of personnel and equipment for response during large scale and long-term crisis.
Exchange of crisis information	Shortcomings in the ability to exchange crisis related information among agencies and organizations.
Evacuation planning & management	Shortcomings in planning and managing large scale evacuation of population in urban areas.

The selection process for these gaps and the current capabilities of the legacy systems of the end-users involved in Trial 4 are described in **D946.11 - Report on Trial Action Plan - Trial 4** (11).

## 4.2 Scenario description of Trial 4

---

The Trial 4 scenario starts from an initial description presented in the Call for Application (CfA):

*A dyke breach is caused by technical failure or by bad weather conditions. A part of the Safety Region Haaglanden, the Netherlands, will be flooded and damaged or destroyed. More than 500.000 people are threatened by the flooding.*

*During the flood, the water level will be about one meter, depending on the exact location of the breach and the altitude of the terrain. The flooding will have significant human and economic impacts. Cascading effects will be:*

- *Flooded roads and railways.*
- *Partly power outage.*
- *(Tele-)communications failure.*
- *Shortages in fresh drinking water and food supply for the population within and outside of the affected area.*

*The scenario requires decisions about the necessity for evacuation of inhabitants of the area afflicted by flooding. A large amount of emergency workers and rescue equipment is needed to deal with the increasing number of exposed people and to manage aforementioned cascading effects. Thus, the situation cannot be handled by Safety Region Haaglanden and regional crisis partners only, but requires deployment of additional evacuation forces, volunteers and resources from national and potentially international networks.*

*When the water has withdrawn, the previously flooded area will be heavily damaged and partly destroyed.*

The scenario covered the threat phase before the flooding as well as the impact phase after the flooding and was split in four different blocks:

- Block 1: threat -48h to -24h before the dyke breach (Cascading effects).
- Block 2: threat -24h to 0h before the dyke breach (Evacuation).
- Block 3: impact 12h to 24h after the dyke breach (Damage assessment).
- Block 4: impact 24h to 48h after the dyke breach (Damage control).

For more details about the scenario of Trial 4 please see **D946.11 Report on Trial Action Plan – Trial 4** (11).

## 4.3 Participating solutions

---

The list of the solutions selected for Trial 4 is presented in Table 4.3. The experience from Trial 1 and 2 has shown that solution providers (especially external solution providers) withdrew their participation in a Trial once they understood the whole effort and complexity of the Trial preparations. Thus, two backup solutions were selected, which would only participate in Trial 4 in case one of other the solutions would be withdrawn. In addition to the selected solutions it was decided that the legacy solution LCMS, which is widely used by Crisis Management organizations in The Netherlands, shall be involved in the Trial.

**Table 4.3: Selected solutions for Trial 4**

Solution name	Solution provider
Airborne and Terrestrial Situational Awareness (consisting of the solutions ZKI and KeepOperational)	DLR / Germany
HumLogSim	WWU / Germany
3Di	Nelen & Schuurmans / Netherlands
SIM-CI	SIM-CI / Netherlands
CrisisSuite	Merlin / Netherlands
<b>BACKUP solutions:</b>	
CrowdTasker	AIT /Austria
Emergency Mapping Tool (EMT)	AIT /Austria
<b>Incumbent solution:</b>	
LCMS	IFV / Netherlands

Table 4.4 provides an overview of the solutions, including their role in Trial 4 and including references to their descriptions in the Portfolio of Solutions.

**Table 4.4: Solutions overview for Trial 4**

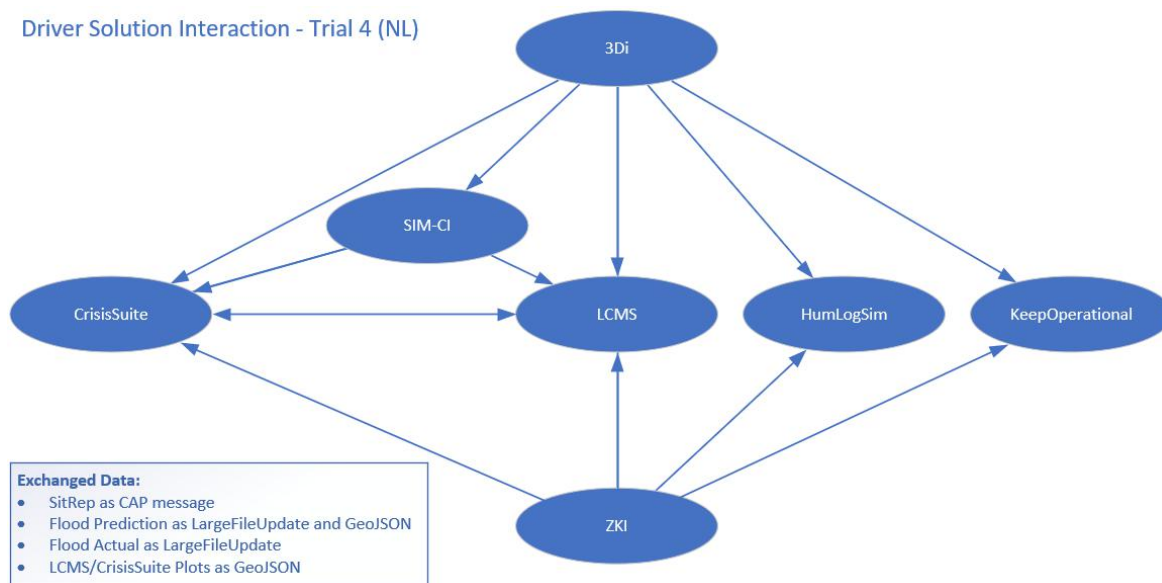
Solution	Short description
Airborne and Terrestrial Situational Awareness (consisting of the solutions ZKI and KeepOperational) <a href="https://pos.driver-project.eu/en/PoS/solutions/24">https://pos.driver-project.eu/en/PoS/solutions/24</a>	Creation of information layers based on aerial images such as traffic analysis and route planning.  In Trial 4, the Terrestrial Situational Awareness solution is used to provide flood masks and flood maps using satellite imagery of the flooded area as well as for the calculation of traffic routes under consideration of flood maps and road blockages.
HumLogSim <a href="https://pos.driver-project.eu/en/PoS/solutions/25">https://pos.driver-project.eu/en/PoS/solutions/25</a>	Performance assessment platform for logistics processes in Crisis Management.  In Trial 4, the HumLogSim solution is used for the calculation of evacuation strategies and the calculation of personnel and logistics.
3Di <a href="https://pos.driver-project.eu/en/PoS/solutions/14">https://pos.driver-project.eu/en/PoS/solutions/14</a>	Simulation software for floods.  In Trial 4, the 3Di solution is used for the calculation of flood scenarios (forecast) and the calculation of the effects of proposed measures including the use of the DEM-edit function.
SIM-CI <a href="https://pos.driver-project.eu/en/PoS/solutions/76">https://pos.driver-project.eu/en/PoS/solutions/76</a>	Visualization of effects if vital infrastructures are affected by a crisis, exchange of information.  In Trial 4, the SIM-CI solution is used for the calculation of cascading effects based on the selected forecast scenarios.
CrisisSuite	Common Operational Picture (map and logbook)

Solution	Short description
<a href="https://pos.driver-project.eu/en/PoS/solutions/22">https://pos.driver-project.eu/en/PoS/solutions/22</a>	<p>In Trial 4, the CrisisSuite solution is used as a COP tool for bi-directional information sharing with LCMS in order to connect also stakeholders from other organizations.</p>
<p>LCMS</p> <p><a href="https://www.lcms.nl/about-lcms">https://www.lcms.nl/about-lcms</a></p>	<p>LCMS is a nation-wide Crisis Management system used in The Netherlands to maintain and share a common operational picture supporting large-scale Crisis Management collaboration. LCMS is used by all 25 safety regions, the majority of the waterboards, Rijkswaterstaat, an increasing number of emergency health care organizations, the Royal Military Police organization and some drinking water providers. LCMS supports net centric collaboration, which is a way of working in which clear agreements are made about sharing information so that decision-making under (crisis) circumstances is always based on an up-to-date, consistent and common operational picture. LCMS is a web-based collaboration environment with a very high level of availability. The environment can be used to share information within an organisation as well as between organizations. It supports maintaining and sharing textual information (through LCMS Text (Log)) as well as geographical information and pictures (through LCMS Plot).</p>
<p>CrowdTasker (Backup solution)</p> <p><a href="https://pos.driver-project.eu/en/PoS/solutions/20">https://pos.driver-project.eu/en/PoS/solutions/20</a></p>	<p>CrowdTasker was envisaged as a backup solution for the case that other solution would be withdrawn. Finally, CrowdTasker was not used in Trial 4.</p>
<p>Emergency Mapping Tool (EMT) (Backup solution)</p> <p><a href="https://pos.driver-project.eu/en/PoS/solutions/26">https://pos.driver-project.eu/en/PoS/solutions/26</a></p>	<p>EMT was envisaged as a backup solution for the case that other solution would be withdrawn. Finally, CrowdTasker was not used in Trial 4.</p>



## 4.4 Trial 4 intended solution interaction

This section provides a high-level overview of the intended collaboration of solutions participating in Trial 4.



**Figure 4.1: Trial 4 solution interactions**

Figure 4.1 provides an overview of the intended communication channels between involved solutions in Trial 4. Each of the shown channels is realised via the messaging system provided by the Test-bed.

Table 4.5 gives an overview about how the individual solutions are integrated with the Test-bed on the technical level (which adapter to be used).

**Table 4.5: Solution integration with Test-bed**

Solution	Used Test-bed adapter
Airborne and Terrestrial Situational Awareness (ZKI)	Java adapter
Airborne and Terrestrial Situational Awareness (KeepOperational)	Java adapter
HumLogSim	Java adapter
3Di	Python adapter
SIM-CI	Java adapter
CrisisSuite	REST adapter
LCMS	NodeJS adapter

More details of the realised solution integration and communication channels can be found in the sections below.

## 4.5 Trial preparation and execution

### 4.5.1 Overview

In the Technical Integration Meeting (TIM) the main focus from technical/integration point of view was on:

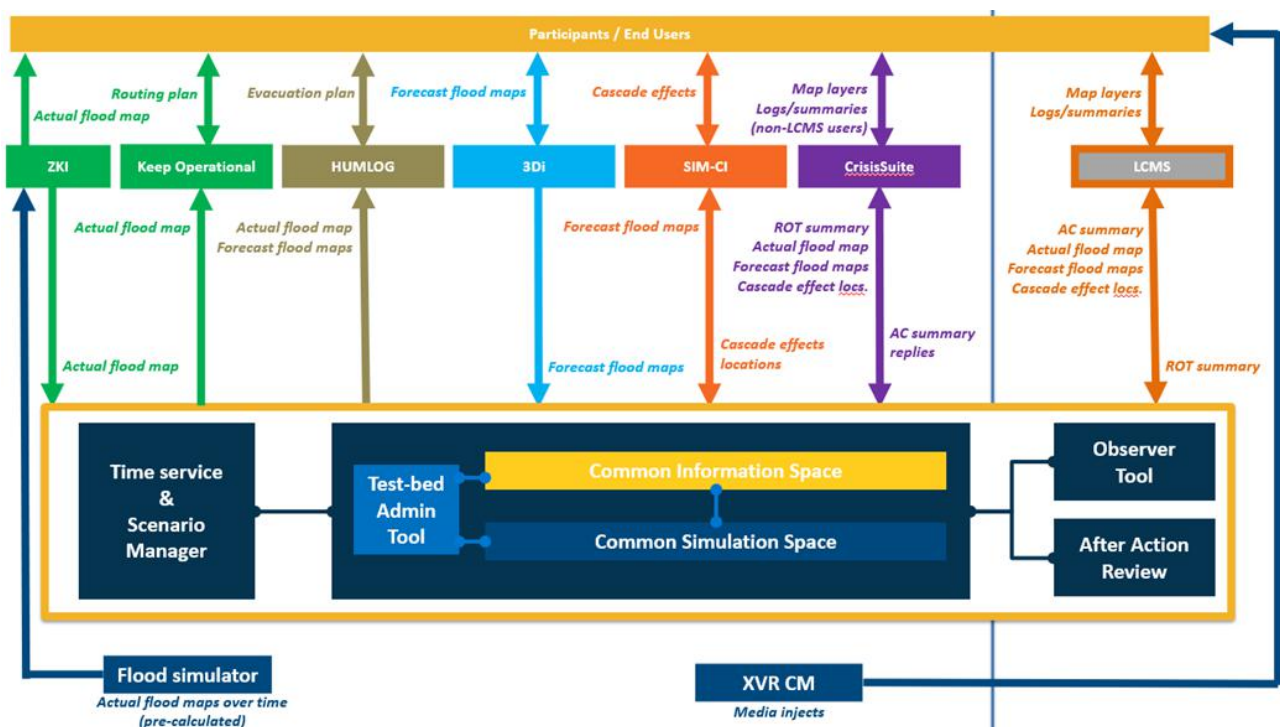
- Discussion of the initial Trial scenario and Trial constraints.
- Presentation of the capabilities of the selected solutions.
- Adaptations of the Trial scenario in order to best explore the solutions capabilities.
- Use of each solution in the scenario, potential data exchange and user group per solution.
- Creation of first data exchange diagrams between solutions, Test-bed and simulation.
- Required adaptations and data conversions in order to enable this data exchange.

The interaction between solutions in Trial 4 is implemented using the following Crisis Management related standards:

- Common Alerting Protocol (CAP) (12).
- GeoJSON (13).
- GeoTIFF (LargeFileUpdate) (14).

These standards are related to the representation of information. They support the exchange of structured information between various solutions. Their implementation was made possible by the fact that the Test-bed reference implementation (8) implements these standards as well and is thus able to receive them, send them and verify their structure.

Figure 4.2 shows the final version of the information exchange diagram for all solutions which was initially created during the TIM and continuously refined afterwards until DR2. To be mentioned is the fact that LCMS is the incumbent solution currently used by several Crisis Management organisations in The Netherlands. This diagram visualises which information is provided/consumed by individual solutions and which information the solutions exchange with participants (end users) on one hand and amongst them (via the Test-bed infrastructure) on the other hand.



**Figure 4.2: Information exchange diagram for the Trial 4 solutions**

Based on the information exchange diagram, the data exchange via the DRIVER+ Test-bed was analysed, and a simplified integration diagram was created (see Figure 4.3) taking into account the capabilities and constraints of the Test-bed.

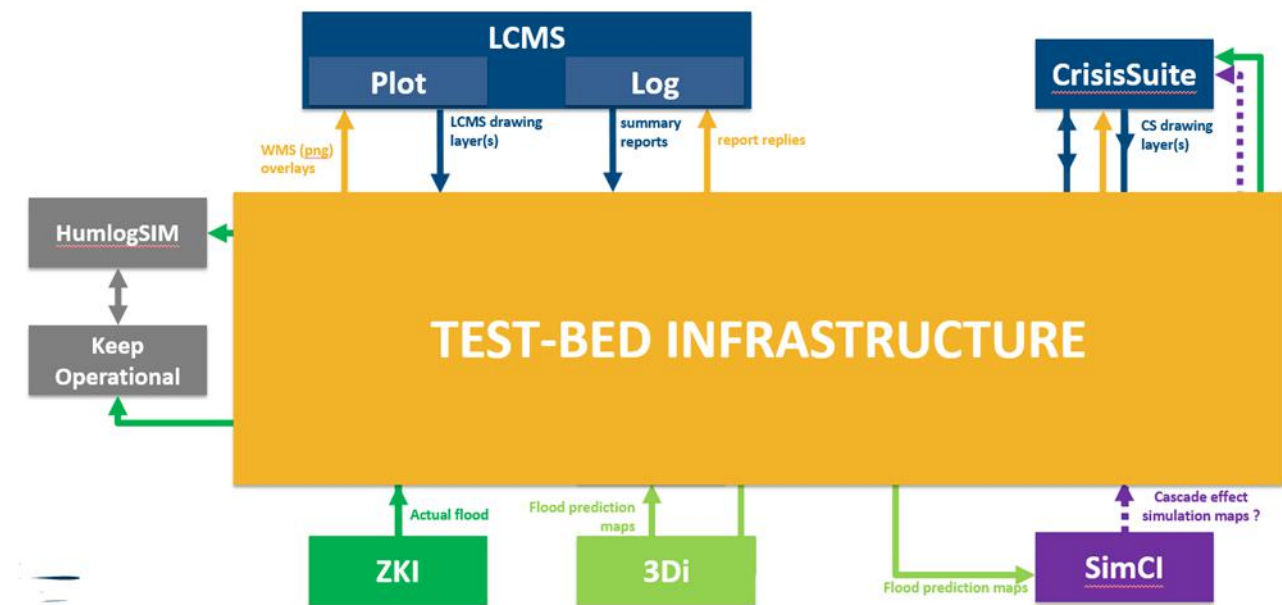


Figure 4.3: Trial 4 data exchange via Test-bed

Taking this diagram as a baseline, the data flow within the Test-bed was analysed and Figure 4.4 was created, visualising the concrete data flows within the Test-bed (mainly for inter-connecting the legacy LMCS with other solutions). An analysis of the data formats available and supported by all involved solutions showed that a GeoTIFF to GeoJSON converter was needed for the foreseen data exchange as shown in Figure 4.4. The GeoTIFF to GeoJSON converter was finally created by TNO before DR1.

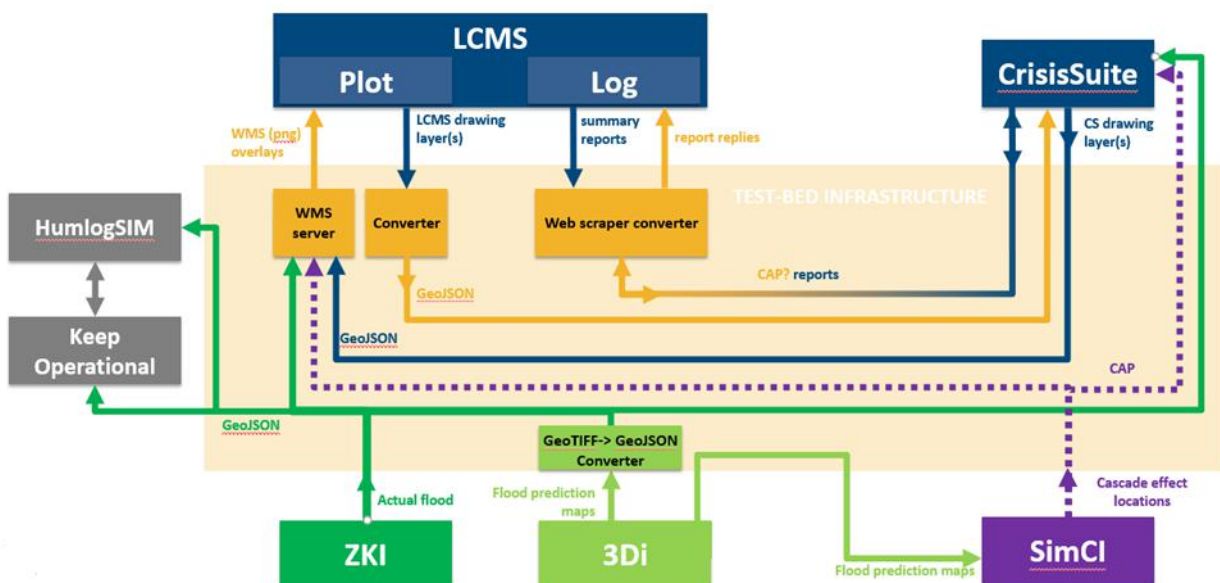


Figure 4.4: Trial 4 data flow within the Test-bed

After the TIM, the focus from technical/integration perspective was on:

- Start of the general integration of all involved solutions into the Test-bed in order to enable a generic data exchange.



- Elaboration of a detailed sequence diagram (UML diagram) per solution (pre-condition was the definition of the use cases per player in the scenario).
- Elaboration of detailed test cases following the sequence diagram for each solution (as sub-elements of the overall Trial scenario).
- Performing the detailed test cases individually per solution provider in remote testing sessions.
- Requirements for multiple instances (and hardware) for solution deployment.
- Preparation for DR1 which shall verify that all test cases for all solutions work correctly following the complete Trial scenario.
- Execution of DR1 and DR2.

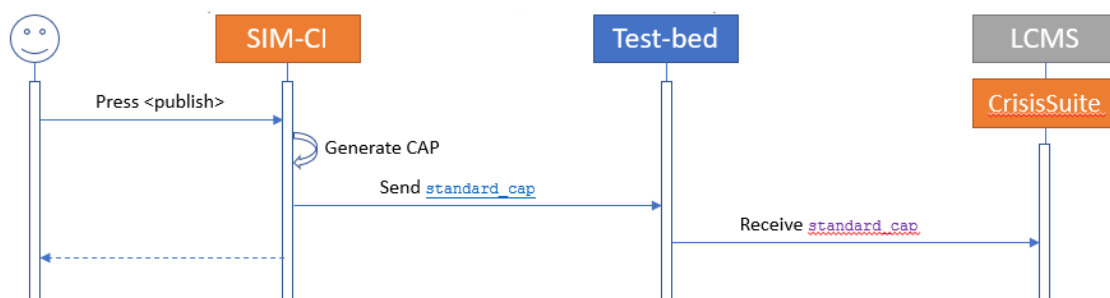
#### 4.5.2 Use cases

The use cases for Trial 4 have been elaborated on the basis of the scenario described in detail in the Trial Action Plan (11) and summarized in section 4.2 above. The information workflow between different solutions during each individual phase of the scenario has been analysed and is presented in this section. The elaborated use cases are listed in Table 4.6. For use cases that include interactions between several solutions, sequence diagrams are sketched in the figures below Table 4.6, providing more details about these interactions.

**Table 4.6: Use cases per solution in Trial 4**

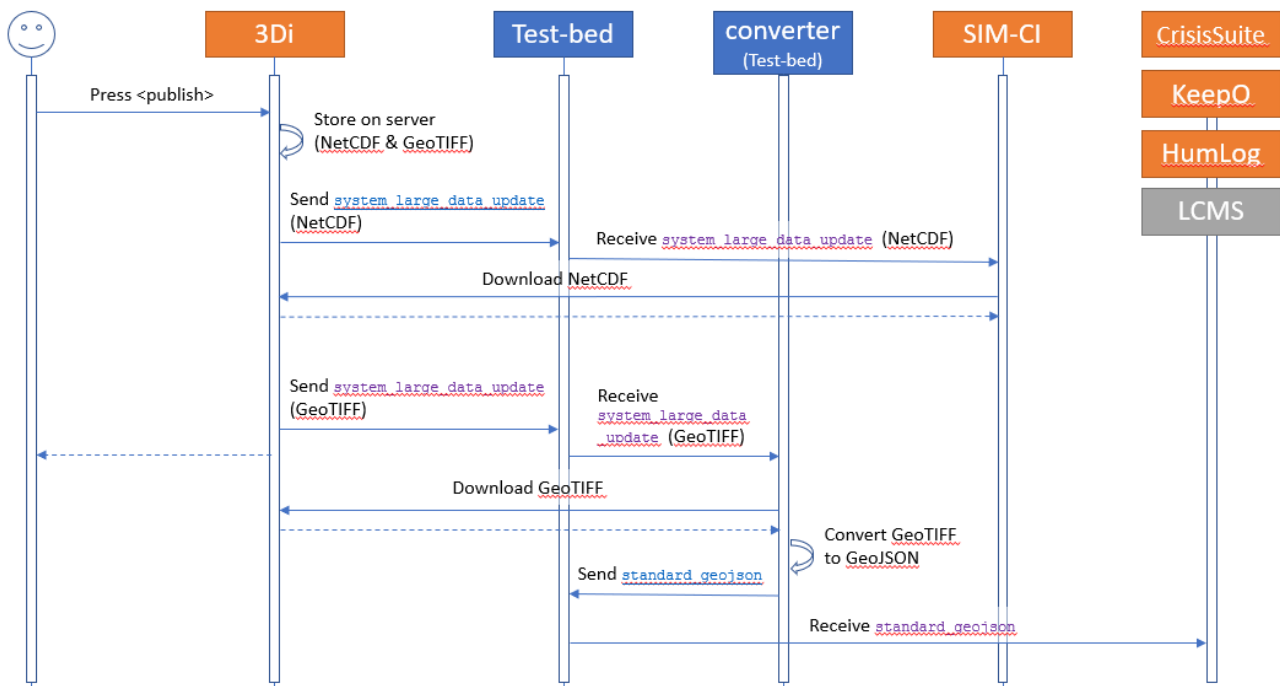
Solution	Use case	Remark
<b>SIM-CI</b>	Enable/disable data layers.	SIM-CI internal use case
	Play out prediction.	SIM-CI internal use case
	Select scenario.	SIM-CI internal use case
	Create screenshots.	SIM-CI internal use case
	Publish info.	See Figure 4.5.
<b>3Di</b>	DEM alterations.	3Di internal use case
	Visualise alternatives.	3Di internal use case
	Publish flood map prediction.	See Figure 4.6.
<b>CrisisSuite</b>	Display map layers.	CrisisSuite internal use case
	Adding/editing summary/overview.	CrisisSuite internal use case
	Publish map layers.	See Figure 4.7.
	Publish summary/overview.	See Figure 4.8.
<b>ZKI</b>	Requesting current flood map.	See Figure 4.9.
	Requesting damage assessment.	ZKI internal use case
<b>KeepOperational</b>	Adding/manipulating/deleting blockades.	KeepOperational internal UC
	Selecting flood scenario.	KeepOperational internal UC
	Planning routes.	KeepOperational internal UC
	Obtaining accessibility information.	KeepOperational internal UC
<b>HumLogSim</b>	Alter evacuation objectives.	HumLogSim internal use case
	Provide shift plan.	HumLogSim internal use case

Solution	Use case	Remark
	Assess/update evacuation plan.	See Figure 4.10.
LCMS	Display map layers.	LMCS internal use case
	Adding messages.	LMCS internal use case
	Publish map layers.	See Figure 4.11.
	Publish summary/overview.	See Figure 4.12.



**Figure 4.5: Use case: Sim-CI – Publish Info (electricity, drinking water, telecom, traffic congestion, vulnerable buildings)**

Figure 4.5 illustrates how SIM-CI distributes information about electricity, drinking water, telecom, traffic situation, vulnerable buildings, etc. SIM-CI encodes this information in standard CAP format and hands it over to the Test-bed. LMCS and CrisisSuite are subscribed at the Test-bed for this kind of information; so they receive the CAP data from the Test-bed.

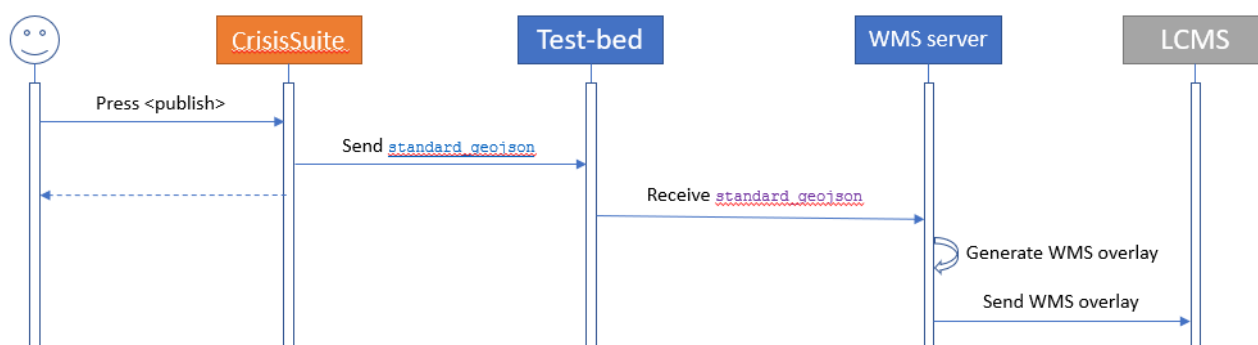


**Figure 4.6: Use case: 3Di – Publish flood map prediction**

Figure 4.6 describes how flood prediction maps are being distributed by the 3Di solution, making use of the Test-bed and associated converter tools. The use case begins when a new flood prediction map is available:

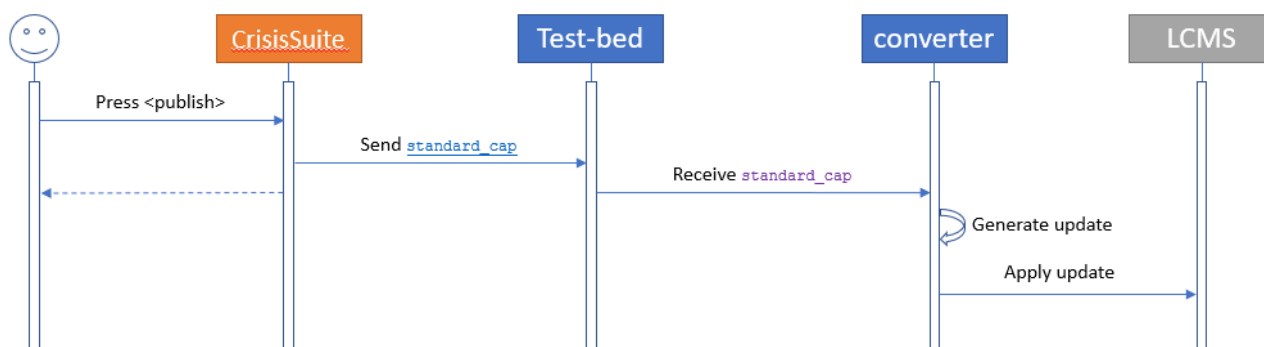
at this time, the 3Di solution stores the map in two formats: NetCDF and GeoTIFF. Then it sends a LargeDataUpdate message to the Test-bed, indicating that a new NetCDF format map is available. The SIM-CI solution is subscribed at the Test-bed for this kind of information, so SIM-CI receives the indication from the Test-bed. SIM-CI, when receiving the indication about a new available NetCDF map, downloads the map by directly accessing the 3Di solution.

Upon storing the new flood prediction map, 3Di also sends a second LargeDataUpdate message to the Test-bed, indicating that a new GeoTIFF format map is available. The converter process is subscribed at the Test-bed for this kind of information, so the converter receives the indication. The converter, when receiving the indication about a new available GeoTIFF map, downloads the map by directly accessing the 3Di solution. The converter then translates data from GeoTIFF into GeoJSON format and sends the GeoJSON message to the Test-bed. Solutions CrisisSuite, KeepOperational, HumLog and LMCS are all subscribed at the Test-bed for receiving GeoJSON messages, so they all will be updated by the new map data.



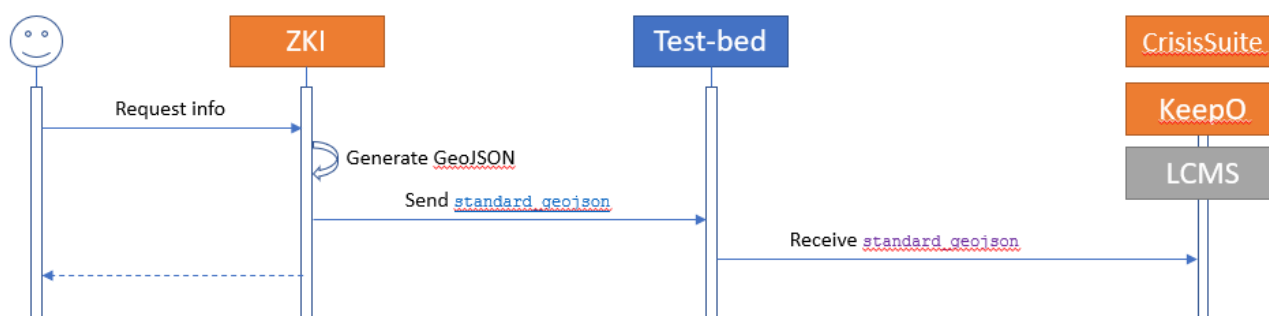
**Figure 4.7: Use case: CrisisSuite – Publish map layers**

Figure 4.7 illustrates the way how CrisisSuite solution shares map layers with the LMCS solution, by support of the Test-bed and the WMS server: CrisisSuite publishes GeoJSON format messages, which are forwarded to the WMS server by the Test-bed. The WMS server generates WMS overlay out of these messages. Finally, the LMCS solution uses the WMS overlay provided by the WMS server. The exchange of similar information in the opposite direction is shown in Figure 4.11.



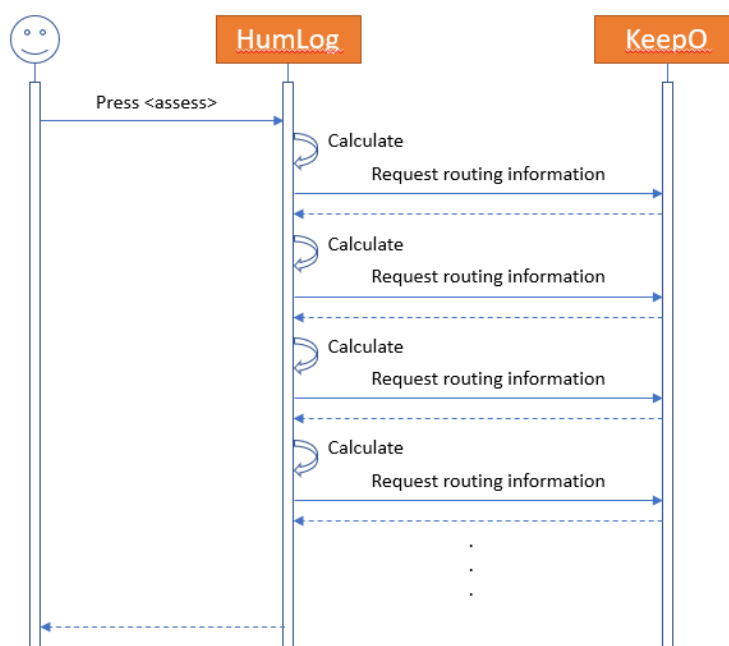
**Figure 4.8: Use case: CrisisSuite – Publish summary/overview**

Figure 4.8 illustrates the way how CrisisSuite solution shares summary/overview information with the LMCS solution, by support of the Test-bed and Converter process: CrisisSuite publishes standard CAP format messages, which are forwarded to the Converter by the Test-bed. The Converter generates updates out of these messages. Finally, the LMCS solution uses the updates provided by the Converter. The exchange of similar information in the opposite direction is shown in Figure 4.12.



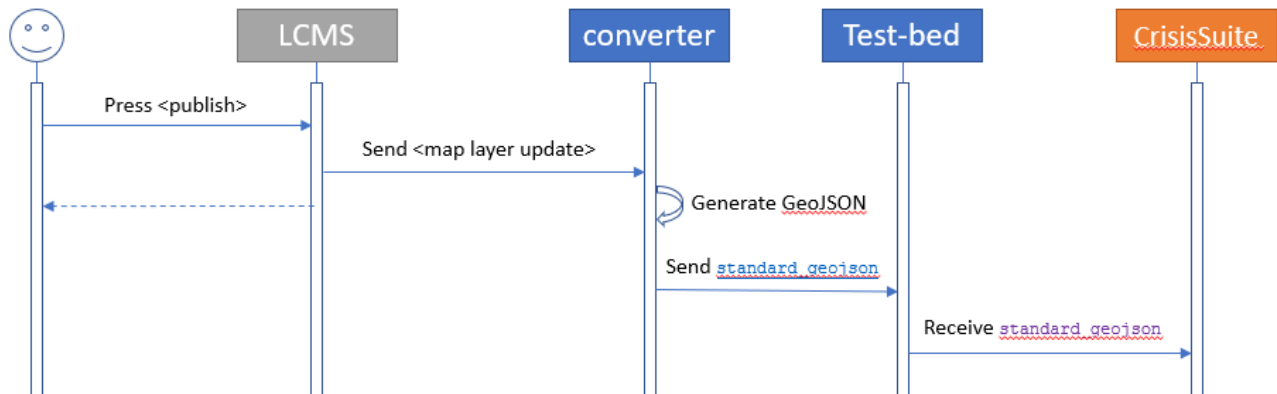
**Figure 4.9: Use case: ZKI – Publish current flood map**

Figure 4.9 gives an overview about the publication of current flood maps. When a new flood map is available (e.g., provided by the simulator), the ZKI solution generates a GeoJSON format message and publishes this message to the Test-bed. Solutions CrisisSuite, KeepOperational and LMCS are subscribed at the Test-bed for GeoJSON messages with current flood maps, therefore they receive these messages.



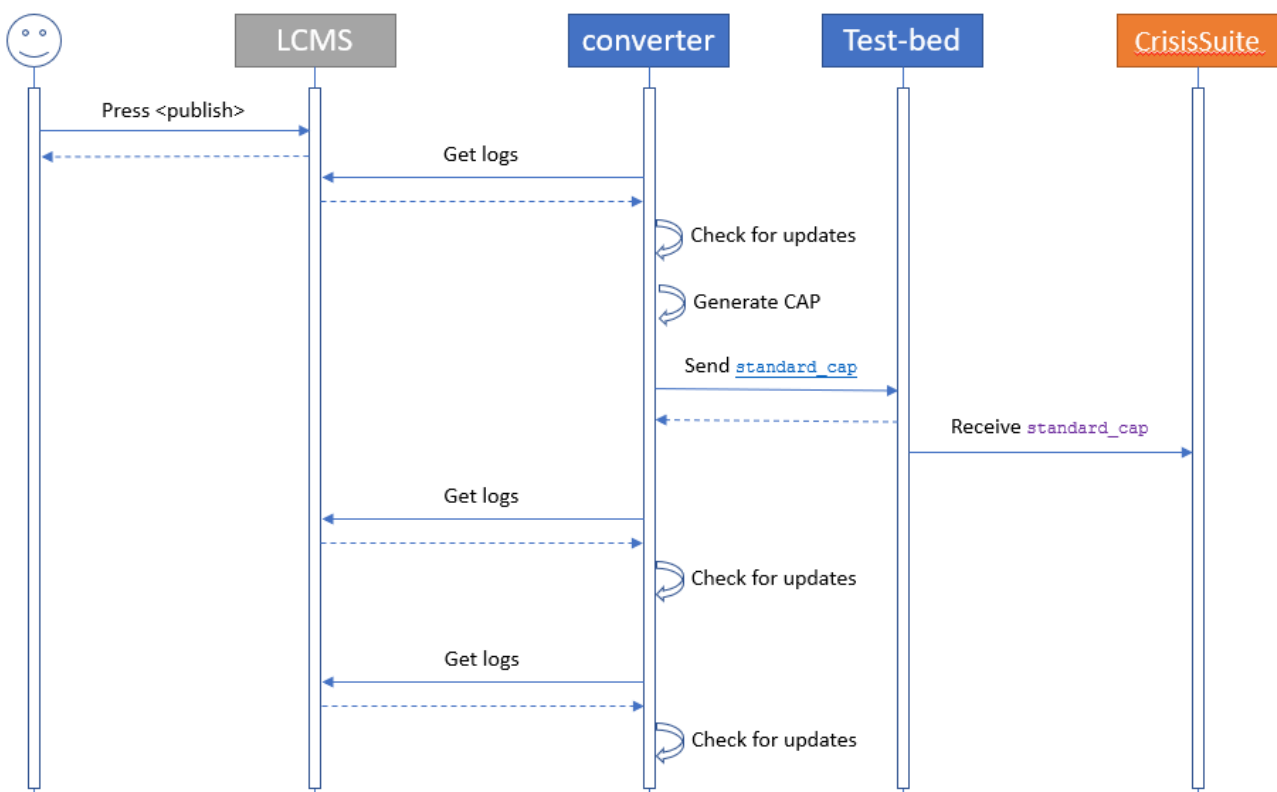
**Figure 4.10: Use case: HumLogSim – Assess/Update evacuation plan**

Figure 4.10 illustrates the information flow between HUMLOG and KeepOperational solutions for the purpose of evacuation planning. The Assessment is performed in the HUMLOG solution, with the support of routing information that is being repeatedly requested directly (without Test-bed interaction) from the KeepOperational solution. In order to maintain routing information up-to-date, HUMLOG sends periodical requests to get the current routing information.



**Figure 4.11: Use case: LMCS – Publish map layers**

Figure 4.11 illustrates the way how the LMCS solution shares map layers with the CrisisSuite solution, by support of the Test-bed and the converter process: LMCS provides map layer updates to the converter, who generates GeoJSON format messages out of it, which are forwarded to the Test-bed. The CrisisSuite solution is subscribed at the Test-bed for this kind of GeoJSON message and therefore receives these messages. The exchange of similar information in the opposite direction is shown in Figure 4.7.



**Figure 4.12: Use case: LMCS – Publish summary/overview**

Figure 4.12 illustrates the way how the LMCS solution shares summary/overview information with the CrisisSuite solution, by support of the Test-bed and Converter process: The converter process actively polls the LCMS for getting updates. If updated information is available, the Converter generates standard CAP messages and publishes them to the Test-bed. CrisisSuite is subscribed for standard CAP format messages at the Test-bed, therefore it receives these messages. The exchange of similar information in the opposite direction is shown in Figure 4.8.

### 4.5.3 Test cases

During DR1 and DR2 about 30 test cases were performed and evaluated. Some of these test cases are not relevant for solution integration, as they only involve operations performed at or with a single solution. Only a sub-set of the test cases involve two or more solutions, or a solution and the Test-bed. Table 4.7 lists this sub-set of test cases, as they are the ones to be investigated and evaluated with respect to solution integration.

**Table 4.7: Test cases related to solution integration performed in Trial 4 DR1 and DR2.**

Test-case	Action centre	Using solution	Description	Receiving action centres	Via solution
1.2.1	Waterboard	3Di	Publish flood map prediction.	HTM Stedin	SIM-CI
1.2.2	Waterboard	3Di	Publish flood map prediction.	Fire Medical Police Municipality Evacuation	LCMS
1.2.3	Waterboard	3Di	Publish flood map prediction.	HTM Stedin International Organizations	CrisisSuite
1.2.4	Waterboard	3Di	Publish flood map prediction.	Police	KeepOperational
1.2.5	Waterboard	3Di	Publish flood map prediction.	Evacuation	HumLog Sim
1.4	Fire / Medical / Police / Municipality / Evacuation / Waterboard	LCMS	Publish map layers.	HTM Stedin International Organizations	CrisisSuite
1.6	Fire / Medical / Police / Municipality / Evacuation / Waterboard	LCMS	Publish logs/summary/overview.	HTM Stedin International Organizations	CrisisSuite
1.9.1	HTM / Stedin	SIM-CI	Publish cascading effect info.	HTM / Stedin	CrisisSuite
1.9.2	HTM / Stedin	SIM-CI	Publish cascading effect info.	Fire Medical Police Municipality Evacuation	LCMS

Test-case	Action centre	Using solution	Description	Receiving action centres	Via solution
1.11	HTM / Stedin	CrisisSuite	Publish map layers.	Fire Medical Police Municipality Evacuation	LCMS
1.12	HTM / Stedin	CrisisSuite	Publish logs/summary/overview.	Fire Medical Police Municipality Evacuation	LCMS
3.2.1	Waterboard	ZKI	Publish current flood map information.	HTM Stedin	SIM-CI
3.2.2	Waterboard	ZKI	Publish current flood map information.	Fire Medical Police Municipality Evacuation	LCMS
3.2.3	Waterboard	ZKI	Publish current flood map information.	HTM Stedin International Organizations	CrisisSuite
3.2.4	Waterboard	ZKI	Publish current flood map information.	Police	KeepOperational
3.2.5	Waterboard	ZKI	Publish current flood map information.	Evacuation	HumLog Sim

A technical data exchange diagram summarizing which kinds of data have been exchanged between which solutions in the scope of which test cases is provided in Figure A3.1 in Annex 3.

#### 4.5.4 Solution integration results

Map centric solutions play a central role in the integration process as they are the medium of choice to display results from other solutions which can be geo-referenced. Using a map as the primary information layer opens the possibility to achieve a very structured presentation of information, with similar information types grouped in layers which can individually be switched on and off for best visibility of information. The availability of layers also depends on the role of the user (e.g. one user group in Trial 4 was not allowed to see all layers of the COP). The overall information flow diagram in Figure 4.13 shows the involved solutions and the information exchanged among them.

Although they look similar, there is a difference in the meaning of the sequence diagrams here and in previous sections. While the diagrams shown in 4.5.2 were used to specify the integration needs during the elaboration phase, the figure here presents the final result.

The top part of the diagram shows the publication of flood prediction data by the 3Di solution. 3Di provides flood prediction information in two different formats (NetCDF, GeoTIFF). Instead of directly publishing this

information, 3Di informs the Test-bed via “LargeDataUpdate” message, whenever an updated version of the flood prediction data is available. Sim-CI solution is subscribed at the Test-bed to receive the information about updated NetCDF data. When receiving the indication of new available NetCDF data, Sim-CI directly downloads the NetCDF data from 3Di. Other solutions interested in the flood prediction update require the data in GeoJSON format. For this reason, the Test-bed, upon receiving the “LargeDataUpdate” message with the indication of a new available GeoTIFF file, downloads the file from 3Di, converts the data into GeoJSON format and publishes the GeoJSON message to subscribed solutions HUMLOG, KeepOperational, Crisis-Suite and LMCS.

The middle part of the diagram shows how map information is being exchanged between the two major map-based solutions in this Trial: between Crisis-Suite and LMCS. Crisis-Suite publishes mapping information in form of map layers in GeoJSON format. Out of the GeoJSON messages, the Test-bed infrastructure generates WMS overlay information, which is used by LMCS to display information originating from Crisis-Suite. In the other direction, the Test-bed generates GeoJSON out of map layer information from LMCS and publishes the GeoJSON to Crisis-Suite.

SIM-CI provides information about the supply status of electricity, drinking water, telecom, traffic congestion, etc. in standard CAP format to the Test-bed. The Test-bed publishes this data without conversion to subscribed solutions Crisis-Suite and LMCS.

The bottom part of the diagram shows the publication data flow for simulated actual flood data. The Flood Simulator triggers the ZKI solution (without involvement of the Test-bed) to indicate an update of the flood information. ZKI generates flood maps information in GeoJSON format and forwards them to the Test-bed. The Test-bed publishes this data without conversion to subscribed solutions Keep-Operational, Crisis-Suite and LMCS.



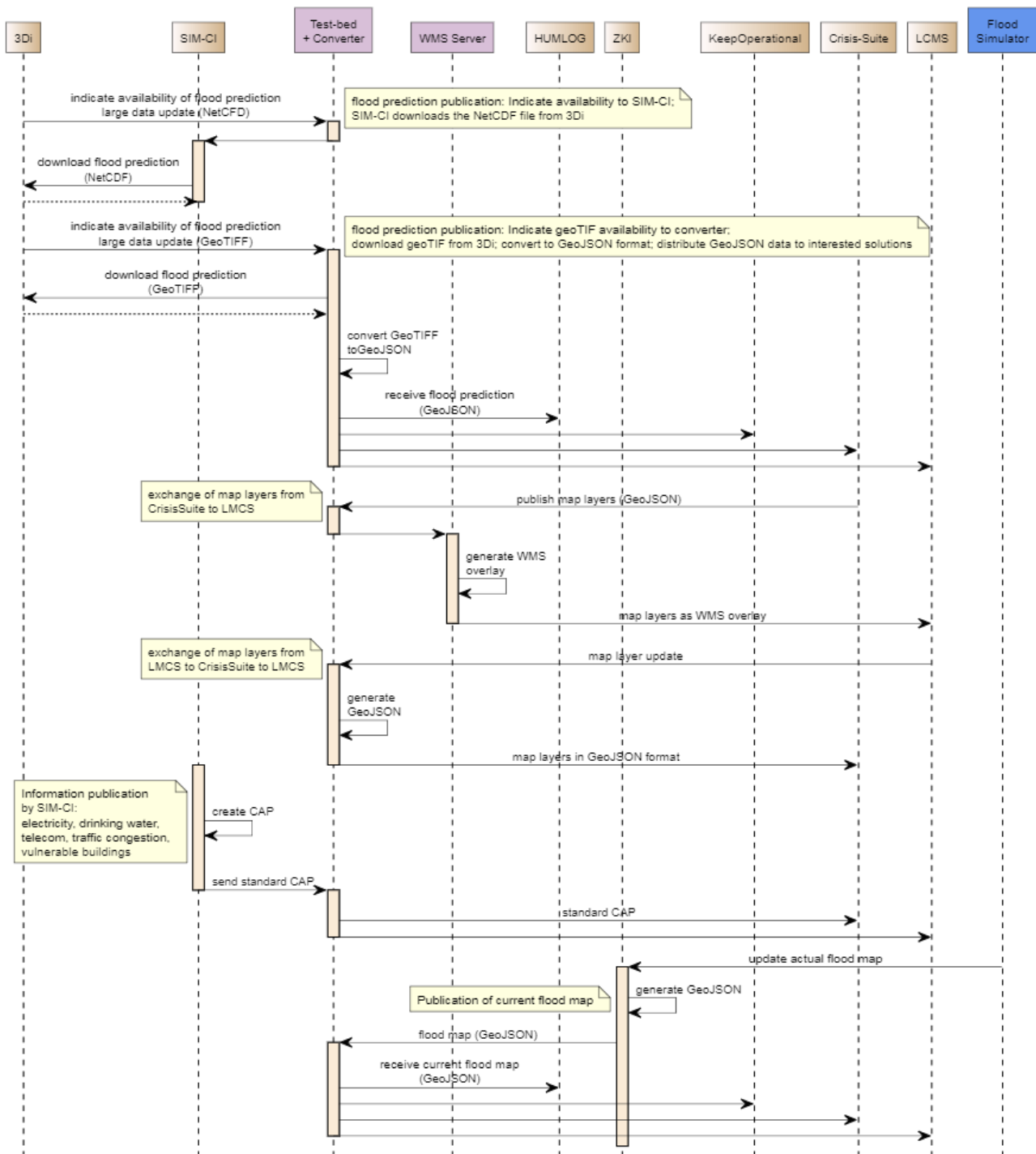


Figure 4.13: Overall information flow sequence diagram for Trial 4

#### 4.5.4.1 Test-bed integration details

The Test-bed components used in Trial 4 were:

- The Test-bed itself.
- The Admin Tool.
- The Trial Management Tool.
- The GeoTIFF/GeoJson gateway.
- The Observer Support Tool (offline mode).
- After-Action Review Tool (AAR Tool).

The Test-bed facilitates data exchange between solutions by so-called “topics”, which are pre-configured communication channels in the Test-bed, allowing broadcast/multicast communication (one solution sends data, many solutions may listen to these data) as well as point-to-point communication between dedicated solutions. On one hand, each solution may publish messages of a certain type onto certain topics; on the other hand, each solution may subscribe at certain topics in order to receive all messages that are published on that topic. More details can be found in Figure A3.3 in Annex 3.

#### 4.5.4.2 Results of the test cases

The validation exercise consists of the consecutive execution of the test cases described in section 4.5.3.

Table 4.8 provides an overview of the test cases and test results achieved in DR1 and DR2. All test scenarios could be successfully tested either in DR1 or in DR2.

**Table 4.8: Test cases and test results achieved in DR1 and DR2**

Test Case	Title	Number of Messages	DR1	DR2
1.2	Publish flood map prediction.	9	OK	OK
1.4	Publish map layers.	22	OK	OK
1.6	Publish logs/summary/overview.	22	partly	OK
1.9	Publish cascading effect info.	0 <sup>4</sup>	OK	OK
1.11	Publish map layers.	3	partly	OK
1.12	Publish logs/summary/overview.	171	yes	OK
3.2	Publish current flood map information.	1	OK	OK

The column “Number of Messages” in the above table refers to the number of messages captured and recorded by the AAR tool during the execution of Trial 4.

The columns DR1 and DR2 indicate which test cases could successfully be executed during Dry Run 1 and Dry Run 2, respectively. The table shows that some test cases were not fully successful during the first Dry Run, but all of them could be performed during the second Dry Run.

## 4.6 Solution providers’ adaptations and integration technical details

This section contains descriptions of each solution provider regarding the adaptations which were needed in the solution to enable the support of the Trial 4. Necessary adaptations are described in terms of UI (User Interface) adaptations as well as back-end adaptations, i.e. changes that were made in controllers and the design of the Test-bed connection.

---

<sup>4</sup> For some reason, no messages from SIM-CI to CrisisSuite have been captured in the AAR tool. The reason for this has to be investigated.

#### 4.6.1 Airborne and Terrestrial Situational Awareness

The integration, adaptation and test effort for the Airborne and Terrestrial Situational Awareness solutions for Trial 4 was as described in this section.

For both modules of the DLR solution “Airborne and Terrestrial Situation Awareness” (i.e. KeepOperational and ZKI) the Java Test-bed adapter was applied.

A local Test-bed instance was deployed and step 0 of the Test-bed integration process was performed. The normally used KeepOperational web-front-end was substituted with an adapter so that the Test-bed can access the underlying services directly. Currently the adapter supports the isochronous routing as well as the regular routing. The messages are in a customised schema because they are quite solution specific and meant to substitute the user interface.

For the Test-bed integration a new adapter was created so that the Test-bed can directly connect to the underlying services of the Airborne and Terrestrial Situation Awareness solution. For the Trial specific implementation DLR aimed at adding a Dutch translation to the front-end of the solution.

The following two test cases have been performed to verify a successful step 0 with regard to Test-bed integration:

- Test case: connecting routing component of KeepOperational to the Test-bed.
  - Start adapter with back-end of KeepOperational-scenario and Test-bed configured.
  - Adapter produces a test event for a routing request (format: keep\_operational\_routing\_request-value.avsc).
  - Adapter subscribes to the topic keep\_operational\_routing\_request.
  - Adapter sends a test event on the topic keep\_operational\_routing\_request.
  - Adapter receives a test event.
  - Adapter verifies the integrity of the received event.
  - Adapter sends routing request to the back-end of KeepOperational-scenario.
  - Adapter receives routing information from back-end.
  - Adapter verifies that no error has occurred.
  - Adapter sends routing information to Test-bed (topic: keep\_operational\_routing\_response, format: keep\_operational\_routing\_response-value.avsc).
  - Verify that the routing information was received in the Test-bed topic browser.
- Test case: connecting isochrone routing component of KeepOperational to the Test-bed.
  - Start Adapter with back-end of KeepOperational-scenario and Test-bed configured.
  - Adapter produces a test event for an isochrone routing request (format: keep\_operational\_isochrone\_request-value.avsc).
  - Adapter subscribes to the topic keep\_operational\_accessibility\_request.
  - Adapter sends a test event on topic keep\_operational\_accessibility\_request.
  - Adapter receives the test event.
  - Adapter verifies integrity of the received event.
  - Adapter sends isochrone request to back-end of KeepOperational-scenario.
  - Adapter receives isochrone information from back-end.
  - Adapter verifies that no error has occurred.
  - Adapter sends isochrone information to Test-bed (topic: keep\_operational\_accessibility\_response, format: keep\_operational\_isochrone\_response-value.avsc).
  - Verify that accessibility information was received in Test-bed topic browser.

For the Trial-specific Test-bed integration (step 1) a new connection to the adapter has been added so that the Test-bed can update the flood mask used for routing. Furthermore, existing map data (e.g. OpenStreetMap) for the area of The Hague is obtained and added to the DLR database.

Additionally, a second instance of the adapted Java adapter was deployed for the ZKI module. Flood mask test data sets for Magdeburg as well as for The Hague region were uploaded to the ZKI geoserver and provided as OGC Webmapping (WMS) and OGC Web Feature (WFS) Services.

Both adapter instances were deployed independently on different computers and were using their own provider identifiers. Additionally, the certificates for both modules, which were provided by the Test-bed developer team, were applied to ensure the communication with secured versions of the Test-bed.

In many test sessions during the test weeks before and during the test sessions of Dry Run 1, Dry Run 2 and the Trial 4 itself the communication with several unsecured and secured versions were established and tested successfully.

The following test cases have been performed to verify a successful step 1 with regard to the Test-bed integration for both modules of the solution:

- Test case: connecting net-restriction component of KeepOperational to the Test-bed.
  - Start adapter with back-end of KeepOperational-scenario and Test-bed configured.
  - Adapter produces a test event for creation of a new net-restriction (format: keep\_operational\_net\_restriction\_create-value.avsc).
  - Adapter subscribes to topic keep\_operational\_net\_restriction\_create\_request.
  - Adapter sends a test event on topic keep\_operational\_net\_restriction\_create\_request.
  - Adapter receives the test event.
  - Adapter verifies integrity of the received event.
  - Adapter sends a request for a new net-restriction to the back-end of KeepOperational-scenario.
  - Adapter receives response from back-end, containing all currently active net-restrictions.
  - Adapter verifies that the new net-restriction is in the response.
  - Adapter sends information on net-restrictions to Test-bed (topic: keep\_operational\_net\_restriction\_response, format: keep\_operational\_net\_restriction\_response-value.avsc).
  - Adapter produces a test event for deletion of the newly created net-restriction (format: keep\_operational\_net\_restriction\_delete-value.avsc).
  - Adapter subscribes to topic keep\_operational\_net\_restriction\_delete\_request.
  - Adapter sends test event on topic keep\_operational\_net\_restriction\_delete\_request.
  - Adapter receives test event.
  - Adapter verifies integrity of received event.
  - Adapter sends request to delete the net-restriction to back-end of KeepOperational-scenario.
  - Adapter receives response from back-end, containing all currently active net-restrictions.
  - Adapter verifies that the new net-restriction is no longer in the response.
  - Adapter sends information on net-restrictions to Test-bed (topic: keep\_operational\_net\_restriction\_response, format: keep\_operational\_net\_restriction\_response-value.avsc).
  - Verify that information on net-restrictions was received in Test-bed topic browser
- Test case: sending information on availability of ZKI web service layer product to the Test-bed.
  - Start ZKI adapter instance with prepared LargeDataUpdate-message.
  - Start KeepOperational adapter instance with back-end of KeepOperational-scenario and Test-bed configured.
  - KeepOperational adapter instance subscribes to topic flood\_actual.
  - ZKI adapter instance sends information on availability of ZKI web service layer as LargeDataUpdate-message to Test-bed (topic: flood\_actual).
  - Verify that information on availability of ZKI web service layer was received in Test-bed topic browser.
  - KeepOperational adapter instance receives LargeDataUpdate-message.
  - KeepOperational starts download of flood mask from ZKI geoserver and integrates it as new net restriction.
  - Verify that the flood mask was integrated as new net restriction in KeepOperational and visualised properly.

## 4.6.2 HumLogSIM

To develop and test the Test-bed integration, a local Test-bed instance was deployed. Additionally, a thin client was developed, which sends test messages to the local Test-bed to be received by HumLogSIM. Both clients use the Java-adapter, which was updated throughout the development of the Test-bed. HumLogSIM is supposed to receive flood map information via the GeoJSON data format.

Test case: receive flood map test data.

- Start HumLogSIM adapter in the back-end of HumLogSIM and register to the test topic `humlog_floodsim_test`.
- Start thin client adapter to send test message to the `humlogsim_flood_test` topic.
- Verify that the test message was received by the Test-bed in the topic browser.
- HumLogSim adapter receives the test message on the topic `humlogsim_flood_test`.
- Store message to a local cache for later use in the simulation.
- Verify that the test message was received correctly.

After successfully integrating with the local Test-bed instance, HumLogSIM was connected to the DRIVER+ Test-bed to exchange data with related applications. In the context of Trial 4, these are 3Di and ZKI to receive flood map data. The test cases for both related solutions are similar but listen to different topics on the Test-bed.

Test case: receive flood map data from 3Di / ZKI.

- Start HumLogSIM adapter in the back-end of HumLogSIM and register to the test topic `flood_prediction_geojson / flood_actual`.
- Adapter receives a message on topic `flood_prediction_geojson / flood_actual`.
- Store message to a local cache for later use in the simulation.
- Verify that the test message was received correctly and that the format is readable.

All test cases were successfully executed in the integration process.

## 4.6.3 3Di

During Trial 4 the 3Di and Lizard Portal were used in combination with the Test-bed. The usual 3Di web portal was used for flood modelling. The Lizard portal was used as data platform where the stored data could be retrieved. Participating in Trial 4 required integration with the Test-bed (STEP 1), development/adaptation of the 3Di flood model of the Hague (STEP 2) and testing the Test-bed during multiple occasions TIM/DR1/DR2/telco's/Trial4 (STEP 3).

### STEP 1: Integration

The integration with the Test-bed required multiple efforts.

- Developing the Python script for connection with the Test-bed. Within this script multiple extra sub-connections had to be made to meet the agreements.
  - Initial connection with the Test-bed server.
  - API-connection integration with the Lizard portal.
  - Integration of the security requirements.
  - Script to convert the 3Di output on the fly from GeoTIFF to GeoJSON format.
- Testing the connection was done during the TIM/DR1/DR2/telco's/Trial4.

## STEP 2: Adaptation

The Hague flood model had to be created and modified during the trial4 period. This consisted of building a basic model, adjusting the model to the needs of the DRIVER+ Trial owners, users and the other solution providers.

- The basic model was built in cooperation with the waterboard Delfland.
- Based on the need of a faster flood model, the model was downsized.
- Based on the need of flooding a point of interest, a part of the digital elevation used for the model was lowered. This is done in consultation with the waterboard and the Veiligheidsregio Haaglanden.
- The model tests were conducted during the TIM/DR1/DR2/telco's/Trial4.

## STEP 3: Testing

After being connected with the Test-bed and adapting the flood model the Test-bed setup, with all solution providers integrated, was tested multiple times (during TIM/DR1/DR2/Telco's). The execution of these tests was done the same way:

1. Get connected with the unsecured Test-bed.
2. Get connected with the secured Test-bed.
3. Run 3Di flood model.
4. Store 3Di results.
5. Send results (GeoTIFF & NetCDF) to the Test-bed.

### 4.6.4 SIM-CI

The SIM-CI tool was augmented with:

- The option to select a location or feature of interest which results in a pop-up showing:
  - Relevant information about the location or feature.
  - Location in RD coordinates.
  - A button to send a geo/time-referenced message or report to the Test-bed.
  - A button to enable the user to enter a text message and to submit the message to the Test-bed connection process containing.
- An indicator which shows the availability of new simulation results.

The intended process is:

- 3Di publishes new data and sends a message into the Test-bed.
- The designated Test-bed connection process or SIM-CI operator processes the 3Di flood mask and imports it into the SIM-CI platform and runs a new simulation.
- All Action Centres (ACs) that have the SIM-CI tool are notified of the newly available results and can open the newest results into their client software.
- Each AC can go through the entire prediction (by moving a time-slider) and select any place of interest in the region.

The AC member can send a message using the SIM-CI tool into the Test-bed to report a certain issue, using the above-mentioned method.

The following is a short overview of the testing and integration that was conducted. The whole process incorporates automated tests starting at the staging environment all the way to the production environment. Out of the many activities performed, the list below summarises the most important steps for the Trial 4.

#### Test-bed integration:

- In the cloud-based solution the REST adapter of the Test-bed was integrated.
- Fully automatic unit-testing including round-trip tests of messages were built in.
- The service can be deployed in a Dry Run mode, where nothing is forwarded to the Test-bed but log it for testing purposes.
- Cloud-native services like this are very resilient and have almost no downtime.
- 100% uptime-check performed in the week before the Trial.
- Final tests run in the tests before the Trial in the Trial week, in cooperation with the technical staff of the Trial/XVR.

#### Specific driver build of client:

- For the Trial a specialised version of the client software was released.
- Features include better user interface, developed and tested with test-users.
- The user-interface is also tested through a series of automatic unit-tests.
- More reliable network interfacing was built in to handle the internet bottleneck at the Trial.
- The simulated, artificial internet was throttled to test the low-internet availability use-case for the Trial, successful test.

#### Specific client models and user accounts for the DRIVER+ project:

- Several unique client models were released for the Trial.
- Close contact with HTM for example resulted in a tram-routing analysis tool, where the availability on the trams w.r.t. power and flooding status was monitored.
- All the models include a wide range of unit- and integration tests.
- All Trial users received login accounts for the Trial.
- All accounts were tested manually for Dry Run 2 and the Trial.

#### Specific Trial production environment launched and scaled to perform smoothly:

- A new production environment was launched several weeks prior to the Trial, during Dry Run 2.
- Full feature tests are automatically run on every new release.
- Full user tests were done before the Trial by own staff.
- Dry Run 2 found several points of improvement which were added on as automatic tests. This was fixed before the Trial.
- Test-bed connection tested manually in three separate testing sessions.

#### Message service to LCMS/CrisisSuite via Test-bed built in client:

- A message service from the software client to the Test-bed was build.
- Automatic tests make sure the client-to-cloud connection operates as intended.
- The CAP-message format was tested peer-to-peer with CrisisSuite on multiple occasions.
- Extensively tested with users between Dry Run 2 and the Trial.

#### Flooding input testing:

- The connection with 3Di was testing in a series of test-runs.
- Connection to their API was verified.
- Retrieval from Test-bed was tested.
- Conversion scripts to import 3Di flooding data were updated in joined discussion.
- Post-conversion the data is automatically verified against a schema and tested for integrity on several parameters.



Test-cases ran as full integration test:

- Together with 3Di the full Trial solution was tested on three test flooding scenarios in The Hague.
- The modified height map was imported from 3Di into the cloud environment.
- Correctness of flooding information in the client was verified with 3Di flooding experts.
- Cascading effects were verified with internal team experts for all use cases.
- For HTM, the cascading effects on the tram network were discussed with the experts from HTM.
- Data consistency was tested with a series of automated tests.

#### 4.6.5 CrisisSuite

The changes performed for Trial 4 are provided below. Due to the fact that CrisisSuite was already used in an earlier Trial (Trial 2), fewer adaptations were required in comparison to other solutions.

- Sending and receiving GeoJSON through the Test-bed. The functionality to receive GeoJSON through the Test-bed both from 3Di and ZKI for the predicted and the actual flood maps was developed, as well as from the LCMS. Next to that the functionality to send any data that has been drawn by a CrisisSuite user into the Test-bed as GeoJSON, to be received by the LCMS was also developed.
- Highlighting of sitrep changes, in order to spot updates differences between the current sitrep and the previous sitrep more easily.
- Store the extent of the map view upon save, in order to render the same view when a user returns to the map after storing in previously.
- Enable styling of icons and polygons in the map view.
- Add pop-up notification for updates on the map through an external source (the Test-bed).

For most of these functionalities unit tests were created in order to automatically verify the correct response of the code to the given input.

#### 4.6.6 LCMS

As initial step, a local Test-bed was deployed in order to start the LCMS connector tool. The LCMS connector was connected to this locally running Test-bed in order to run the tests.

Test cases:

- It was checked with the topics-UI interface of the Test-bed that heartbeat-messages were being sent from the LCMS-connector. This implies that:
  - A connection with the Test-bed was set-up correctly.
  - The connector produced messages with the correct client ID.
  - The connector was able to send a message to system topics of the Test-bed.
- It was checked that the LCMS-connector was able to send GeoJSON data over the `lcms_plot` topic. By achieving this, it showed that:
  - The connector was able to send a message to a Trial topic.
  - The sent data followed the format defined in the `named-geojson avro` schema.
- It was checked that the LCMS-connector could read information from LCMS and publish it on the `standard_cap` topic, proving that:
  - The connector can read informational messages from LCMS.
  - Convert those to a CAP-message format.
  - Convert those to a message matching the `standard_cap avro` schema
  - Publish that message on the Test-bed.



- It was checked that the LCMS-connector could publish data from the Test-bed to LCMS, by:
  - Receiving a message from the standard\_cap topic.
  - Converting the message from the CAP-format to a readable format used by LCMS.
  - Obtain the desired receiver information from the message (e.g. HTM or Stedin).
  - Publishing the message to LCMS in to the respective receive tab.
- It was checked that the LCMS-connector could connect to a secure Test-bed by:
  - Configuring a certificate, user name and password.
  - Connecting to the Test-bed.
  - Sending a message to the standard\_cap topic.
  - Receiving a message from the standard\_cap topic.

Next to the local tests, all the tests have also been performed in several other meetings, where the LCMS-connector was connected with the external Test-bed and communicated with the other solutions.

## 5. Final Demo

This section describes the main activities related to the integration of solutions for the Final Demonstration and the resulting outcomes.

The general purpose of the Final Demonstration was double. After four DRIVER+ Trials conducted successfully, the first aim of the Final Demonstration was to demonstrate the trialling process, but the Final Demonstration was more than a demonstration it was a Trial itself, and one of the most complex in terms of scenario. The focus of the Final Demonstration was the exchange at the highest level of coordination, between ERCC (Emergency Response Coordination Centre) and EUCPT (EU Civil Protection Team) during a crisis in a country located outside of EU where the EUCP Mechanism is activated and civil protection modules from several member states are deployed. The multinational aspect was one of the key aspects of the Final Demonstration which involved players located in Poland and Netherlands.

The Trial was organized by SRC and SGSP and was conducted as a table-top Trial at the premises of SGSP (Warsaw), SRC (Warsaw) and SRH (The Hague).

The Final Demo had one preceding technical integration meeting (TIM) and three preceding Dry Runs (named DR1, DR2 and DR2½) in order to prepare the Trials properly, both from a technical and an organizational perspective. The dates and locations the TIM, DRs and the Final Demo are listed in Table 5.1.

**Table 5.1: Dates and locations of TIM, DR1, DR2 and Final Demo**

Event	Duration	Date	Location
TIM	2 days	27-28/03/2019	Ispra, Italy
Dry Run 1	5 days	24-28/06/2019	Ispra, Italy
Dry Run 2	5 days	23-27/09/2019	Warsaw, Poland
Dry Run 2 ½	2 days	28-29/10/2019	online
Final Demo	5 days	25-29/11/2019	Warsaw, Poland + The Hague, Netherlands

### 5.1 CM gaps addressed in the Final Demonstration

According to the DRIVER+ deliverable **D922.11 List of CM gaps** (2) three gaps were defined and served as a basis for the definition of the scenario and the selection of solutions. Table 5.2 lists these gaps.

**Table 5.2: CM gaps addressed in the Final Demo**

Name	Gap description
Shortcomings in interoperability	Shortcomings in the ability to exchange crisis-related information among agencies and organisations.
Lack of “Common Operational Picture”	Lack of a “Common Operational Picture” environment to integrate data sources and calculation results from different models crucial for decision making process from the perspective of the incident commander.
Limits in the ability to merge and synthesize disparate data sources	Limits in the ability to merge and synthesize disparate data sources and models in real time (historic events, spreading models, tactical situation, critical assets map, etc.) to support incident commander decision making

## 5.2 Scenario description

The Final Demo scenario covered a forest fire with cascading effects (discovery of an unknown refugee camp in the forest):

*Large Forest Fires (FF) are spreading in a fictional, non-EU country “Driverstan”. National response capabilities of country “Driverstan” are not sufficient to manage the FF. Request for assistance is prepared by country “Driverstan” and EUCPM is activated. Modules and assets are offered by the Member States. Upon acceptance of the modules, country “Driverstan” National Disaster Management Agency (NDMA) is working closely with EUCPT on site.*

*Upon arrival, EUCPT identifies another important issue: large unofficial refugee settlement is endangered by fire spread and in upcoming days it will be necessary to evacuate it (and defend it from the fire during the evacuation). Unexpected need to relocate thousands of refugees adds to overall complexity and results in stronger EU-UN cooperation.*

The scenario was focused on international information exchange among the EUCP Modules, EUCPT (closely linked to TAST) and NDMA as well as situation reporting to ERCC.

## 5.3 Participating solutions

5 solutions participated in the Final Demonstration. Table 5.3 lists the solution names and the solution providers.

**Table 5.3: Selected solutions for the Final Demonstration**

Solution name	Solution provider
CrisisSuite	Merlin / Netherlands
SOCRATES OC	GMV / Spain
viewTerra Evolution	VWORLD / France
Drone Rapid Mapping	Hexagon/Creotech / Poland
Field Reporting Tool	JRC / Italy

Table 5.4 provides an overview of the solutions, including their role in the Final Demonstration and including references to their descriptions in the Portfolio of Solutions.

**Table 5.4: Solutions overview for the Final Demonstration**

Solution	Short description
CrisisSuite  <a href="https://pos.driver-project.eu/en/PoS/solutions/22">https://pos.driver-project.eu/en/PoS/solutions/22</a>	CrisisSuite is a tool that supports the net centric working methods of crisis teams by creating a universal picture of the crisis and shares it horizontally and vertically with other teams in the crisis organization.  In the Final Demonstration, the CrisisSuite solution is used to <ul style="list-style-type: none"> <li>• Create/update logs and situation reports.</li> <li>• Obtain information relevant for reports.</li> <li>• Receive and visualize geo-information.</li> </ul>

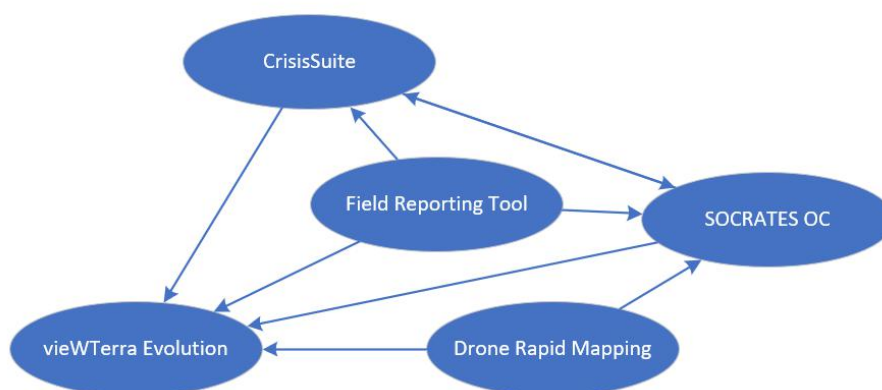
Solution	Short description
<p>SOCRATES OC</p> <p><a href="https://pos.driver-project.eu/en/PoS/solutions/12">https://pos.driver-project.eu/en/PoS/solutions/12</a></p>	<p>SOCRATES OC enhances analysis and decision-making capabilities by improving shared situational awareness based on relevant information about the operational situation including crisis events, missions and resources.</p> <p>In the Final Demonstration, the SOCRATES OC solution is used to</p> <ul style="list-style-type: none"> <li>• Visualize Common Operational Picture (COP).</li> <li>• Publish incident updates.</li> </ul>
<p>viewTerra Evolution</p> <p><a href="https://pos.driver-project.eu/en/PoS/solutions/94">https://pos.driver-project.eu/en/PoS/solutions/94</a></p>	<p>viewTerra Evolution is a 4D Earth Viewer as well as a data &amp; assets integration and development platform allowing Civil responders to build a virtual 4D representation (3D synthetic environment + Time dimension) of a potential Crisis area to provide a Common Operational Picture.</p> <p>In the Final Demonstration, the viewTerra solution is used to</p> <ul style="list-style-type: none"> <li>• Visualize high resolution Digital Elevation Map (DEM).</li> <li>• Receive and visualize drone imagery data on 3D map.</li> <li>• Receive and visualize geo-tagged photos on 3D map.</li> <li>• Receive and visualize Geo-information from legacy system Copernicus.</li> <li>• Measure elevation.</li> </ul>
<p>Drone Rapid Mapping</p> <p><a href="https://pos.driver-project.eu/en/PoS/solutions/21">https://pos.driver-project.eu/en/PoS/solutions/21</a></p>	<p>Drone Rapid Mapping enables rapid mapping of incident/crisis area. The solution enables fast generation of orthophoto maps based on imagery acquired by any drone (RPAS) available to rescue or Crisis Management actors.</p> <p>In the Final Demonstration, the DRM solution is used to publish incident drone imagery.</p>
<p>Field Reporting Tool</p> <p><a href="https://pos.driver-project.eu/en/PoS/solution/141">https://pos.driver-project.eu/en/PoS/solution/141</a></p>	<p>The Field Reporting Tool (FRT) is a platform to collect and promptly share multimedia georeferenced information.</p> <p>In the Final Demonstration, the DRM solution is used to</p> <ul style="list-style-type: none"> <li>• Obtain photos by capturing them from XVR on scene display.</li> <li>• Publish geo-tagged photos.</li> </ul>

## 5.4 Final Demo intended solution interaction

This section provides a rough overview of the intended integration of solutions participating in the Final Demo.

Figure 5.1 provides an overview of the intended communication channels between involved solutions in the Final Demo. Each of the shown channels is realised via the messaging system provided by the Test-bed.

## Driver Solution Interaction – Final Demonstration



**Figure 5.1: Final Demo solution interactions**

Table 5.5 gives an overview about how the individual solutions are integrated with the Test-bed on the technical level (which adapter to be used).

**Table 5.5: Solution integration with Test-bed**

Solution	Used Test-bed adapter
CrisisSuite	REST adapter
SOCRATES OC	Java adapter
vieWTerra Evolution	REST adapter
Drone Rapid Mapping	Python adapter
Field Reporting Tool	REST adapter

More details of the realised solution integration and communication channels can be found in the sections below.

## 5.5 Final Demo preparation and execution

### 5.5.1 Overview

Figure 5.2 shows the final version of the overall solution interaction diagram, which evolved during the integration process. It illustrates the information exchanged between involved solutions in the Final Demo by making use of the Test-bed technical infrastructure.

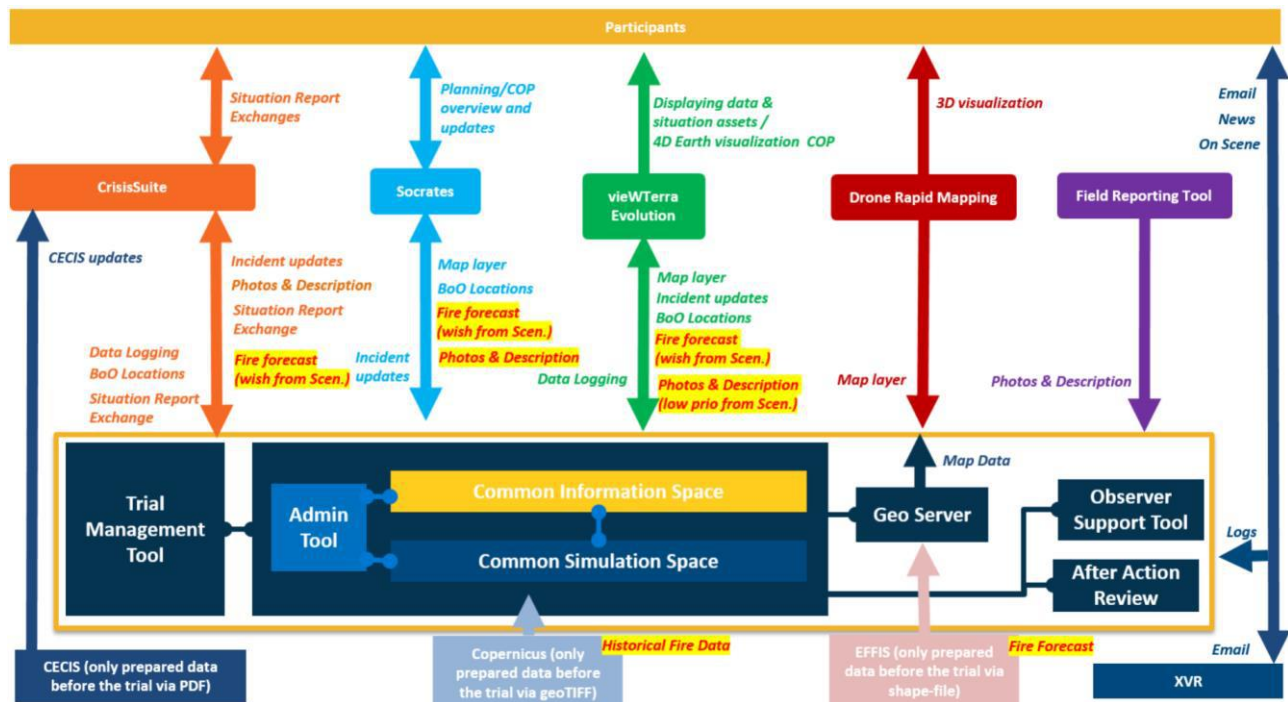


Figure 5.2: solution interaction diagram for the Final Demo

## 5.5.2 Use cases

Table 5.6 provides an overview of the usage of solutions and their interactions in the Final Demo.

Table 5.6: Use of solutions in the Final Demo

Users	Solution	Use case	Input from	Output to
Modules	SOCRATES OC	Map situation update & assessment.		All sharing SOCRATES OC Map (EUCPT, Modules) and CrisisSuite.
Modules	CrisisSuite	Reporting.		EUCPT
Modules	CrisisSuite	Log keeping.		Own Logbook, Modules/EUCPT Logbook.
Modules	viewTerra Evolution	3D Terrain analysis.		
Modules	viewTerra Evolution		Field Reporting Tool	Visualisation of Field reports.
EUCPT	SOCRATES OC	Situation description & assessment.		All sharing SOCRATES OC Map (EUCPT, Modules) and CrisisSuite.
EUCPT	CrisisSuite	Reporting.		ERCC.
EUCPT	CrisisSuite	Log keeping.		Own Logbook, Modules/EUCPT Logbook, EUCPT/ERCC Logbook.
EUCPT	CrisisSuite	Information sharing.		ERCC and Modules.
ERCC	CrisisSuite	Log keeping.		

Users	Solution	Use case	Input from	Output to
ERCC	CrisisSuite	Information sharing.		CrisisSuite, EUCPT.
ERCC	SOCRATES OC	Map situation update.		All sharing SOCRATES OC (not initially planned, used after request of ERCC).
MEDEVAC	CrisisSuite	Log keeping.		

### 5.5.3 Test cases

This section describes the test cases that have been defined for the validation of Final Demo solution integration. Table 5.7 lists these test cases, ordered by solution.

**Table 5.7: Final Demo solution integration test cases.**

TC	Acting solution	Test Case Description	Peer (Test-bed or solution)
4.1.1	SOCRATES OC	Connect with the Test-bed.	Test-bed
4.1.2	SOCRATES OC	Send CAP Message with Module situation (EXCH_REQ_105).	CrisisSuite, vieWTerra Evolution
4.1.3	SOCRATES OC	Send UPDATE CAP message with Module situation (EXCH_REQ_11x).	CrisisSuite, vieWTerra Evolution
4.1.4	SOCRATES OC	Send CANCEL CAP Message.	CrisisSuite, vieWTerra Evolution
4.1.5	SOCRATES OC	Read DRM maplayer Message.	Drone Rapid Mapping
4.1.6	SOCRATES OC	Read FRT CAP Messages (INFO_EXCH_REQ_140).	Field Reporting Tool
4.1.7	SOCRATES OC	Read Cs and TMT staff map Message.	Test-bed CrisisSuite
4.1.8	SOCRATES OC	Read in Test-bed Icon Server Icons.	Test-bed
4.2.1	Field Reporting Tool	Connect with the Test-bed.	Test-bed
4.2.2	Field Reporting Tool	Send CAP message with geo-localised images (EXCH_REQ_120).	SOCRATES OC, CrisisSuite, vieWTerra Evolution
4.2.3	Field Reporting Tool	Send CAP message with geo-localised file.	SOCRATES OC, CrisisSuite, vieWTerra Evolution
4.3.1	CrisisSuite	Connect with the Test-bed.	Test-bed
4.3.2	CrisisSuite	Send BoO message via CAP MAP staff mapp Message.	
4.3.3	CrisisSuite	Send CS_INTERNAL Message.	N.A.
4.3.4	CrisisSuite	Send LOG Message Sitrep.	Test-bed
4.3.5	CrisisSuite	Send LOG Message Logbook.	Test-bed



TC	Acting solution	Test Case Description	Peer (Test-bed or solution)
4.3.6	CrisisSuite	Send LOG Message User Action.	Test-bed
4.3.7	CrisisSuite	Read SOCRATES OC situation messages (INFO_EXCH_REQ_130).	SOCRATES OC
4.3.8	CrisisSuite	Read SOCRATES OC UPDATE situation messages (INFO_EXCH_REQ_130).	SOCRATES OC
4.3.9	CrisisSuite	Read SOCRATES OC CANCEL situation message.	SOCRATES OC
4.3.10	CrisisSuite	Read FRT CAP Messages (INFO_EXCH_REQ_140).	Field Reporting Tool
4.3.11	CrisisSuite	Read CS_INTERNAL Message.	N.A.
4.3.12	CrisisSuite	Read TMT CAP Message.	Test-bed
4.3.13	CrisisSuite	Read in Test-bed Icon Server Icons.	Test-bed
4.4.1	Drone Rapid Mapping	Connect with the Test-bed.	Test-bed
4.4.2	Drone Rapid Mapping	Send Map Layer Update message with WMS LinkI (INFO_EXCH_REQ_150).	SOCRATES OC, vieWTerra Evolution
4.5.1	vieWTerra Evolution	Connect with the Test-bed.	Test-bed
4.5.2	vieWTerra Evolution	Read DRM Large data update (INFO_EXCH_REQ_160).	Drone Rapid Mapping
4.5.3	vieWTerra Evolution	Read SOCRATES OC Situation CAP messages (INFO_EXCH_REQ_170).	SOCRATES OC
4.5.4	vieWTerra Evolution	Read SOCRATES OC Situation UPDATE CAP messages (INFO_EXCH_REQ_170).	SOCRATES OC
4.5.5	vieWTerra Evolution	Read SOCRATES OC CANCEL situation message.	SOCRATES OC
4.5.6	vieWTerra Evolution	Read FRT CAP messages (INFO_EXCH_REQ_180).	Field Reporting Tool
4.5.7	vieWTerra Evolution	Read TMT Cap Message.	Test-bed
4.5.9	vieWTerra Evolution	Read in Test-bed Icon Server Icons.	Test-bed

A technical data exchange diagram summarizing which kinds of data have been exchanged between which solutions in the scope of which test cases is provided in Figure A4.1 in Annex 4.

#### 5.5.4 Solution integration results

The UML sequence diagram in Figure 5.3 shows the message exchanged during the execution of test cases for the Final Demonstration.

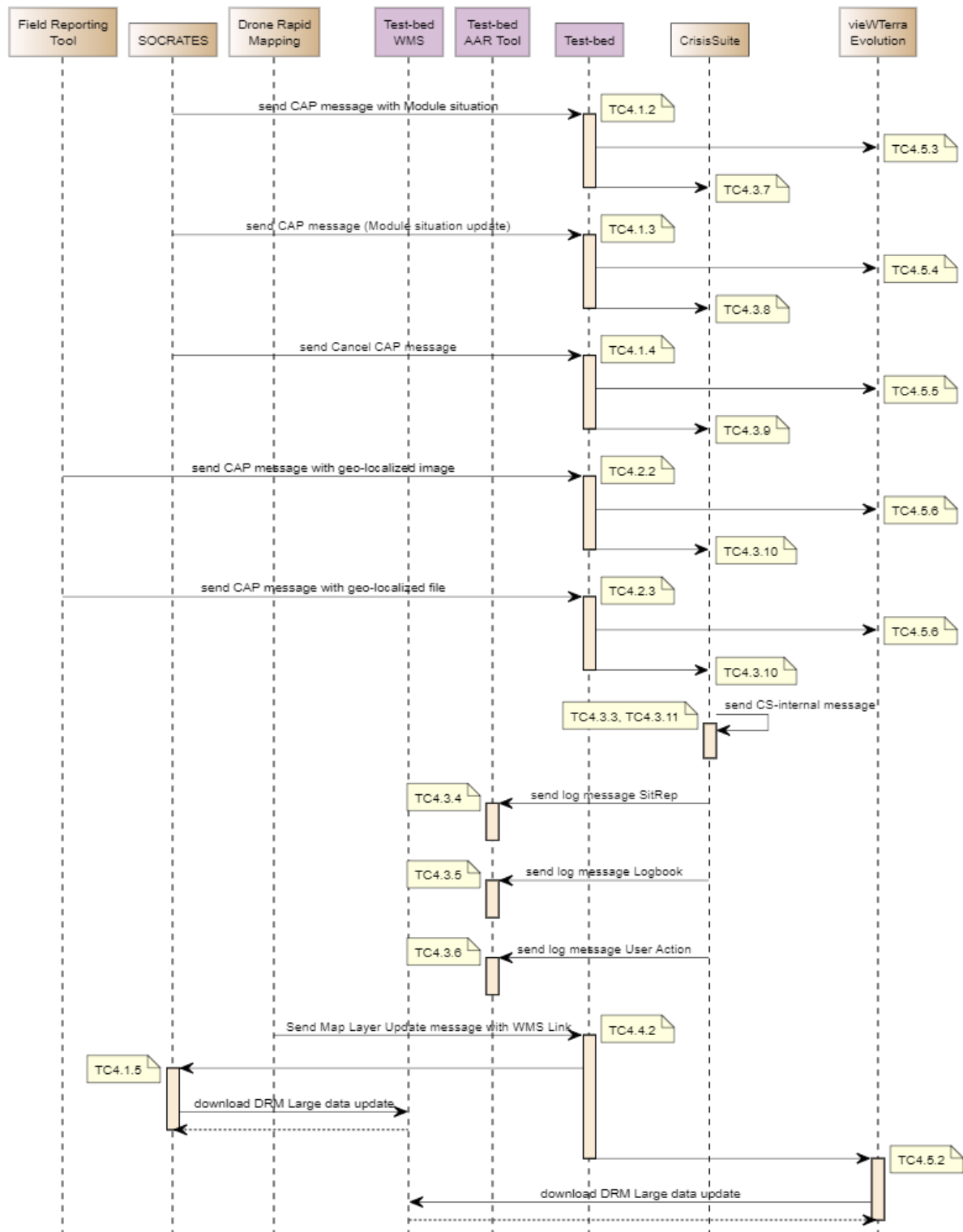


Figure 5.3: Overall information flow sequence diagram for the Final Demo

#### 5.5.4.1 Test-bed integration details

The Test-bed components used in the Final Demo were:

- The Test-bed itself.
- The Admin Tool.
- The Trial Management Tool (TMT).
- The Observer Support Tool (OST).

- After-Action Review tool (AAR).
- The GeoServer.

The Test-bed facilitates data exchange between solutions by so-called “topics”, which are pre-configured communication channels in the Test-bed, allowing broadcast/multicast communication (one solution sends data, many solutions may listen to these data) as well as point-to-point communication between dedicated solutions. On one hand, each solution may publish messages of a certain type onto certain topics; on the other hand, each solution may subscribe at certain topics in order to receive all messages that are published on that topic. More details on the topics used in the Final Demo can be found in Figure A4.3 in Annex 4.

#### 5.5.4.2 Results of the test cases

The validation exercises related to solution integration consist of the execution of the test cases described in section 5.5.2.

Table 5.8 provides an overview of the test results achieved in DR1, DR2 and DR2½. Most of the test cases could be successfully tested in at least one Dry Run. For a few test cases it was decided at the DR2½ to not continue their execution (they are marked with “Dropped” in the DR2½ column).

**Table 5.8: Test results achieved in DR1, DR2 and DR2½ of the Final Demo**

TC	Description	topic	DR1	DR2	DR2½
4.1.1	Connect with the Test-bed.	N.A.	OK	OK	OK
4.1.2	Send CAP Message with Module situation (EXCH_REQ_105).	socrates_map	Partial	OK	OK
4.1.3	Send UPDATE CAP message with Module situation (EXCH_REQ_11x).	socrates_map	Partial	OK	OK
4.1.4	Send CANCEL CAP Message.	socrates_map	Unknown	OK	OK
4.1.5	Read DRM maplayer Message.	system_map_layer_update	Unknown	OK	OK
4.1.6	Read FRT CAP Messages (INFO_EXCH_REQ_140).	frt_map	Unknown	Failed	Dropped
4.1.7	Read Cs and TMT staff map Message.	staff_map	Unknown	Unknown	Dropped
4.1.8	Read in Test-bed Icon Server Icons.	N.A.	Unknown	OK	OK
4.2.1	Connect with the Test-bed.	N.A.	Failed	Partial	OK
4.2.2	Send CAP message with geo-localised images (EXCH_REQ_120).	frt_map	Partial	Partial	OK
4.2.3	Send CAP message with geo-localised file.	frt_map	Unknown	Partial	Partial
4.3.1	Connect with the Test-bed.	N.A.	OK	OK	OK
4.3.2	Send BoO message via CAP MAP staff map Message.	staff_map	Unknown	Partial	Dropped

TC	Description	topic	DR1	DR2	DR2½
4.3.3	Send CS_INTERNAL Message.	cs_internal	Unknown	Unknown	OK
4.3.4	Send LOG Message Sitrep.	system_logging	Unknown	Unknown	OK
4.3.5	Send LOG Message Logbook.	system_logging	Unknown	Unknown	OK
4.3.6	Send LOG Message User Action.	system_logging	Unknown	Unknown	OK
4.3.7	Read SOCRATES OC situation messages (INFO_EXCH_REQ_130).	socrates_map	OK	OK	OK
4.3.8	Read SOCRATES OC UPDATE situation messages (INFO_EXCH_REQ_130).	socrates_map	OK	OK	OK
4.3.9	Read SOCRATES OC CANCEL situation message.	socrates_map	Unknown	OK	OK
4.3.10	Read FRT CAP Messages (INFO_EXCH_REQ_140).	frt_map	Partial	Partial	OK
4.3.11	Read CS_INTERNAL Message.	cs_internal	Unknown	Partial	OK
4.3.12	Read TMT CAP Message.	staff_map	Unknown	Partial	Dropped
4.3.13	Read in Test-bed Icon Server Icons.	N.A.	Unknown	Unknown	OK
4.4.1	Connect with the Test-bed.	N.A.	Failed	OK	OK
4.4.2	Send Map Layer Update message with WMS LinkI (INFO_EXCH_REQ_150).	system_map_layer_update	Failed	OK	OK
4.5.1	Connect with the Test-bed.	N.A.	OK	OK	OK
4.5.2	Read DRM Large data update (INFO_EXCH_REQ_160).	system_map_layer_update	Failed	OK	OK
4.5.3	Read SOCRATES OC Situation CAP messages (INFO_EXCH_REQ_170).	socrates_map	OK	OK	OK
4.5.4	Read SOCRATES OC Situation UPDATE CAP messages (INFO_EXCH_REQ_170).	socrates_map	OK	OK	OK
4.5.5	Read SOCRATES OC CANCEL situation message.	socrates_map	Unknown	OK	OK
4.5.6	Read FRT CAP messages (INFO_EXCH_REQ_180).	frt_map	OK	Unknown	OK
4.5.7	Read TMT Cap Message.	staff_map	Unknown	Unknown	Dropped
4.5.9	Read in Test-bed Icon Server Icons.	N.A.	Unknown	OK	OK

## 5.6 Solution providers' adaptations and integration technical details

---

This section contains descriptions of each solution provider regarding the adaptations which were needed in the solution to enable the support of the Final Demonstration. Necessary adaptations are described in terms of UI (User Interface) adaptations as well as back-end adaptations, i.e. changes that were made in controllers and the design of the Test-bed connection.

### 5.6.1 CrisisSuite

The changes performed for the Final Demonstration are described in this section. Due to the fact that CrisisSuite was already used in earlier Trials (Trial 2 and 4), fewer adaptations were required in comparison to other solutions.

- Allow inclusion of attachments in sitreps (and sending them through the Test-bed).
- Easily aggregate provided sitrep answers from multiple sources into a new sitrep.
- Show image and pdf attachments on the map module (from FRT).
- Displaying of complex geographical map layers (from Socrates) including opacity and icons from an external icon server.
- Differentiating input from Socrates between the ERCC/EUCPT crisis and the EUCPM crisis.
- Location search in the map module.
- Information (CAP) routing from CrisisSuite to CrisisSuite through the Test-bed.
- Logging specific actions inside CrisisSuite to the Test-bed.

### 5.6.2 SOCRATES OC

This section provides an overview about GMV development and integration efforts for the Final Demo.

#### Connectivity and Test-bed

- Development of the SOCRATES OC adapter for the FD, which builds on the DRIVER+'s Java adapter.
- Reception of Map Layer Update messages in order to provide the corresponding notifications to SOCRATES OC.
- Sending of CAP messages containing the operational situation displayed in SOCRATES OC. This includes the transformation of the data provided by SOCRATES OC into the corresponding format as defined by the CAP standard.
- Sending of CAP's CANCEL messages when an event was removed from the operational situation in SOCRATES OC.

#### Development of specific features in SOCRATES OC as required for the Final Demo

- Customization of entity (events and resources) attributes to those required for the Final Demo (including the types of events and resources, nationality of resources, etc.).
- Styles of geometries added to the set of information provided by SOCRATES OC.
- New feature for indicating when a piece of information was relevant for the ERCC.
- Highlighting of icons when the corresponding entity was updated (e.g. update of its position or some of its attributes). Stop highlighting after a predefined period of time or after the user clicks on the icon.
- Retrieval of the icons associated to the different entity types from the DRIVER+ Test-bed's icon server.
- Map search functionality was added (e.g., search by city name, etc.).
- Route planning functionality was added, including the drawing of the route in the map and the listing of the corresponding route indications. Both the name of the location or its specific coordinates can be provided for the origin and destination of the route.
- Predefined types of geometries (e.g. burnout area or module's area of responsibility) were added, so they could be selected by users when creating a new geometry. Each predefined type of geometry had

an associated style (e.g. border and fill colour) and shape (e.g. line, polygon), so there was no need to select them manually by the user.

- Display the nationality of the corresponding resource below its associated icon in the map.
- Show all coordinates in decimal format.
- New feature which allows locating a given map layer in the map according to its bounding box.

#### **Other customization activities for the Final Demo**

- Customization of visible functionality for the Final Demo, keeping only the functionality to be used during the Trial in order to make it easier for practitioners to get familiar to the solution (e.g., mission-related functionality was hidden).
- New feature allowing the creation a new event or resource in a given location by double-clicking on the map.
- Allow grouping and ordering entities in the corresponding event and resource lists according to the new set of attributes used for the Final Demo.
- New feature for automatically adding to the list of map layers available in SOCRATES OC those received through the Map Layer Update messages.
- Size of labels associated to geometries modified dynamically according to the corresponding zoom level.

#### **Preparatory testing sessions**

- In-house offline tests for the new functionality using a local Test-bed.
- Online testing session with vieWTerra solution after the Final Demo's Dry Run 1.
- Online testing sessions before the Final Demo's Dry Run 2.
- Online testing session after the Final Demo's Dry Run 2 (in the scope of the Dry Run 2.5).

#### **Preparation of training material**

- Update of SOCRATES OC User Exercises manual according to the updated version for the Final Demo.
- Preparation of a script for the interactive training session with practitioners, aligned with some of the episodes composing the Final Demo's Trial scenario.

### **5.6.3 vieWTerra Evolution**

This section provides an overview about VWORLD development and integration efforts for the Final Demo.

#### **Connection to Test-bed (on top of already developed for Trial 3)**

- Topics registration: staff\_map, socrates\_map, map\_layer\_update, frt\_map.
- Connection to on-line TB4 Test-bed for Run1.
- Connection to secured on-line TB6 for Trial.

#### **Test-bed messages interfacing**

Writing functions to interface vieWTerra Evolution with messages received from the Test-bed:

- Parsing of JSON in CAP format messages and treatment of potential errors.

According to information parsed, calling of various vieWTerra Evolution SDK functions in order to:

- Add 3D pins & labels for SOCRATES OC, Field Reporting Tool (FRT) & Drone Rapid Mapping (DRM) assets.
- Attach Test-bed messages to pins.
- Add 2D windows for messages information display (sender ID, GPS location, content etc.).
- Display area/zones (coloured polygons & lines including opacity component) defined in SOCRATES OC (displayed either in 2D or 3D mode).
- Display 2D geotagged photos (from FRT).

- Display 2D geotagged PDF files (from FRT).
- Add DRM and GeoServer-supplied WMS 2D Imagery and fire updates streams (Copernicus EMS EFFIS service) in vieWTerra Evolution Layers Tab and allow draping of these over the vieWTerra Evolution 3D terrain.

#### **Development of specific features for the need of Final Demo**

- Trace Window: allowing easy navigation by simple click on message name/info.
- On-the-fly messages Log System, avoiding any potential loss of information in case of system failure.
- Action-Replay System allowing replaying the messages recorded during a session – used for roll-back during FD.
- Icon server access to display and manage Icons (same as accessed by SOCRATES OC and Crisis Suite solutions).
- Hide/unhide feature for each message, allowing the operator to potentially hide/unhide a message.

#### **Provision of specific Databases**

Search for, treatment and integration of databases for Sweden: Enskogen, Grotingen, Hammarstran and Trelleborg, Stockholm, Sveg region:

- 3.6 m RGB Copernicus imagery (very High-Resolution Image Mosaics). Colour treatment and cloud removal.
- 3.6 m and 90cm Copernicus Land Cover (ESM 2012 - 2017 release) colour classification correspondence.
- 90 cm RGB DigitalGlobe imagery: colour treatment and cloud removal.
- 30 m Digital Terrain Models (from mixed satellite source).
- Footprints creation (from Open Street Map source, in order to render and display buildings in 3D (using vieWTerra Evolution auto-extrusion of cities function)).

#### **Sweden Land Cover 30 m + DTM 30 m**

Recent 30 m Land Cover for data artifacts correction in Sweden, and 30m Sweden DTM (no SRTM data above 60° north).

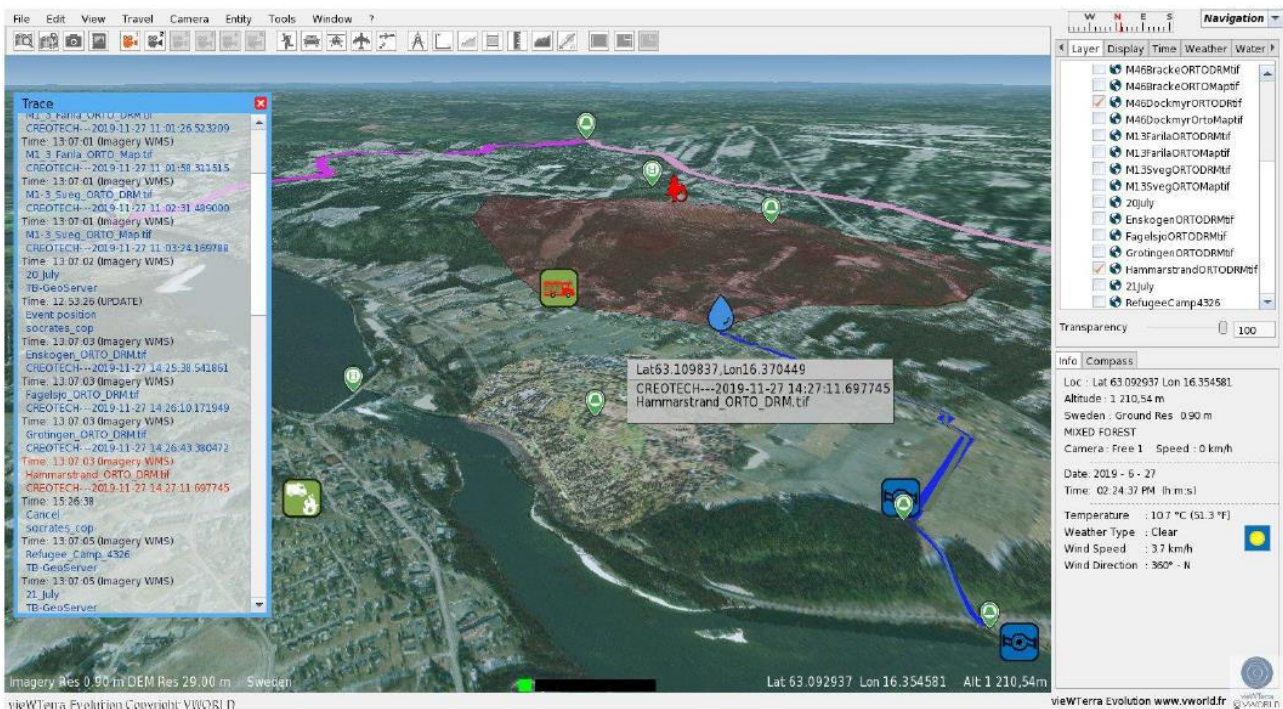
- Sweden Land Cover 30 m: 2,017,984 sq. km.
- Sweden DTM 30 m: 1,282,820 sq. km.
- Trelleborg Region:
  - 15 m Imagery: 27,084 sq. km.
  - 3.6 m Imagery: 1,592 sq. km.
  - 90 cm Imagery: 118 sq. km.
  - 3 m DTM: 2,211 sq. km.
  - 1.5 m DTM: 3,200 sq. km.
  - 70 cm DTM: 30 sq. km.
  - 3.6 m Land Cover: 2,787 sq. km.
  - 70 cm Land Cover: 44 sq. km.
  - Buildings' footprints: 14,300 sq. km.
- Stockholm Region:
  - 3.6 m Imagery: 677 sq. km.
  - 90 cm Imagery: 340 sq. km.
  - 2.5 m DTM: 2,705 sq. km.
  - 3.6 m Land Cover: 2,254 sq. km.
  - 90 cm Land Cover: 1,002 sq. km.
  - Buildings' footprints: 2,953 sq. km.
- Sveg AOI:
  - 3.6 m Imagery: 10,004 sq. km.



- 90 cm Imagery: 1,168 sq. km.
- 3 m DTM: 1,277 sq. km.
- 3.6 m Land Cover: 11,626 sq. km.
- Buildings' footprints: 15,845 sq. km.
- Hammarstrand + Grotigen AOI:
  - 7.2 m Imagery: 11,250 sq. km.
  - 90 cm Imagery: 308 sq. km.
  - 3.6 m Land Cover: 11,312 sq. km.
  - Buildings' footprints: 300 sq. km.

### **Draping and display of local aerial (drone-acquired) 2D Imagery (layer from Drone Rapid Mapping) and integration of drone-acquired 3D models (also from Drone Rapid Mapping):**

- DRM 2D imagery: displayed as WMS layers draped over the viewTerra Evolution 3D terrain using Hexagon WMS server infrastructure.
- DRM photogrammetry-acquired 3D Models (Digital Surface Models): conducting integration tests into the viewTerra Evolution global 3D Terrain (using custom viewTerra Evolution Holes creation functionality). However final decision taken was not to use these ready-made 3D models in the Final Demo Trial.



### **Testing sessions & adjustments**

- In-house off-line tests -on-line testing using secured and un-secured Test-bed versions.

### **Telco meetings participations / TIM, DR1 & 2, DR2½ and Trial participation**

- Average of one 45min to 1-hour telco every 2 weeks / Full participation from TIM to Trial.

### **5.6.4 Drone Rapid Mapping**

This section provides an overview about Creotech development and integration efforts for the Final Demo.

- Re-configuration of the REST adapter of Test-bed allowing for secured connection (with necessary changes to JSON generating scripts).
- Additional features development in alignment to Final Demo Requirements:

- Remote system management and operation possibility, locally by WLAN and over Internet.
- Orthophotomap generation with transparent background.
- Automated WMS, WMTS & .shp generation for newly created orthophotomaps processed from drone imagery.
- Enhanced local presentation of the processing results (orthophotomap, 3D model) in dedicated portal with measurements possibility.
- Possibility to share results and allow multiple accesses to data for remote users connected to the system by WLAN (e.g. allowing independent parallel access to data for field units commanders).
- Browser access – allowing data access and viewing in the portal for users connected by Internet.
- Processing progress monitor with error reporting and logging.
- Enhanced user interface allowing drone data processing setup and start in few simple steps.
- Datasets preparation for the Final Demo as per the Scenario Team requirements (creation of GeoTIFF files and 3D models for the pre-defined locations in Sweden: adjustment to the surroundings and the coordinates change):
  - Sveg, Farila, Hammarstrand, Fagelsjo, Enskogen, Dockmyr, Grotingen, Bracke.
- Replication of the full system configuration and data in the remote environment (intended to serve as a plan B in the case of any technical issues and in fact successfully used during the Final Demo as some IP connectivity problems were faced locally in SGSP).

### 5.6.5 Field Reporting Tool

This section provides an overview about JRC development and integration efforts for the Final Demo.

- Test-bed REST adapter integration in FRT mission workflow. As soon as a mission is published to web-API, it is submitted, as a CAP message, to the adapter. After the first time all other submissions have status Update and refers to the previous one.
- The C# adapter was tested several times without luck and the REST adapter was used.
- Minor Mission CAP message modifications in order to be fully compliant with CAP 1.2 specifications.
- Unauthenticated access to the mission resources in accessible formats.
- Server setup (port openings) and adapter configuration in order to establish the connection between REST adapter and Test-bed (tb3 and secured tb6).
- The mobile device required a specific setup, tested on many devices, in order to work together with the GPS spoofing software that allowed creating contents located elsewhere than the Final Demo.

## 6. Trial independent Test-bed integration of internal (non-selected) solutions

Independently from the Trials and in parallel to their preparation and execution, the DoW indicates that all DRIVER+ internal solutions included and described in the PoS must be integrated in the Test-bed. This shall be done for the sake of readiness in case some of these solutions will be selected in future Trials. Another aspect for this integration is that it will enable an easier evaluation of its Crisis Management functions also beyond the scope of the DRIVER+ project.

### 6.1 DRIVER+ solution categorisation

DRIVER+ solutions can be divided into several groups:

- DRIVER+ internal solutions, which are provided by one of the organisations of the DRIVER+ consortium.
- DRIVER+ external solutions, which are provided by organisations outside the DRIVER+ consortium.

In order to achieve a wider context in the DRIVER+ Trials it was requested by the EC to include on average min. 50% of external solutions in the Trials. External solutions shall – just as internal solutions – be described in the PoS database and undergo the same solution selection process for each Trial.

As a result of this selection process, there is a group of

- DRIVER+ internal solutions, used in Trials (Group A).
- DRIVER+ internal solutions, not used in Trials (Group B).
- DRIVER+ external solutions, used in Trials (Group C).
- DRIVER+ external solutions, not used in Trials (Group D).

For Groups A and C the solution integration into the Test-bed was performed during the preparation phase of the respective Trial, but also for Group B the Test-bed integration was intended to be performed (see explanation in section 6 of **D932.12** (15)). The integration of Group B solutions into the Test-bed was achieved for all solutions except the DEBRIS tool and GDACS mobile. The providers of these 2 solutions did not manage to perform the solution integration within the given timeframe, budget and available resources.

### 6.2 Solutions integration overview

The selection/integration of individual internal and external solutions for individual Trials is summarised in Table 6.1 and Table 6.2.

**Table 6.1: Selection of internal solutions for individual Trials / Final Demo**

Solutions	Trial 1	Trial 2	Trial 4	Trial 3	Final Demo	Non-selected
Social Media Analysis Platform (Thales)						
Airborne and terrestrial situational awareness (DLR)						
CrowdTasker (AIT)						
Humlog (WWU)						
Psychological First Aid (DRC)						
SOCRATES OC (GMV)						

Solutions	Trial 1	Trial 2	Trial 4	Trial 3	Final Demo	Non-selected
Rumour Debunker (AIT)						
Life-X COP (Frequentis)						
MDA Command and Control system (MDA)						
GDACS mobile (WWU)						
Protect (EDISOFT)						
IO-DA (Armines)						
Debris management ()						
EMT (AIT)						
PROCEED (ITTI)						

Table 6.2: Selection of external solutions for individual Trials / Final Demo

Solutions	Trial 1	Trial 2	Trial 4	Trial 3	Final Demo	Non-selected
CrisisSuite						
3Di water management						
Drone Rapid Mapping						
ASIGN						
SIM-CI						
vieWTerra Evolution						

### 6.3 Solution integration achievements

Exchanging data with the Test-bed is a first important step which will support the communication with other solutions via the Test-bed at a later stage and thus speed up the technical preparation process in future Trial activities.

For the DRIVER+ internal solutions not selected for Trials the status of the integration process into the Test-bed, their necessary adaptations and their testing progress is described in the following sections.

In order to integrate solutions into the Test-bed, the following steps have to be performed:

- Understanding the Test-bed concept.
- Understanding the Test-bed adapter options and choosing the right adapter for each solution.
- Understanding the concept of “related solutions” which is another solution to test the data exchange via the Test-bed.
- Defining the messages to be exchanged between 2 related solutions via the Test-bed.
- Connecting the adapter to the solution.
- Exchanging messages between solution and Test-bed according to the integration steps described above and reporting the result of the message exchange via Test-bed.

To support this process an integration information package was created and made available under the following link: <https://github.com/DRIVER-EU/Test-bed#integration-process>.

With this information, solution providers started their Test-bed integration with a local version of the Test-bed and try to connect their solution to one of the available Test-bed adapters.

As all technical support questions and answers related to Test-bed integration were assumed to be of interest for all solution providers, a communication channel was established in form of an online forum with the online communication tool SLACK under the following link: <https://driver-eu.slack.com/messages/C6YQK3FUJ/>.

To describe the benefit of a solution from a practitioner's point of view, so called "use cases" were described. Use case (UC) descriptions of individual solutions enable practitioners an easy understanding of a solutions capabilities by focusing on the added value from an end-user perspective (leaving out technical details). For a technical integration, which enables an automatic data exchange between 2 or more solutions via the Test-bed use case descriptions were extended and described then 2 related solutions exchanging data (UC related solution).

These steps were performed by the solutions listed in the following sections.

### 6.3.1 Rumour Debunker

A description of the Rumour Debunker solution can be found here: <https://pos.driver-project.eu/en/PoS/solution/60>). The following use cases have been defined for the integration of this solution with the Test-bed.

#### **UC1: Continuous media monitoring (quality assured)**

A typical problem which is addressed in use case 1 is that the internet provides a quantity and variety of information. It is impossible to evaluate manually, whether information is true or not.

For example, in a flooding event in Austria, someone posted on social media that cholera bacteria are in the water - which was not true. There is a dramatic increase in methods observable for fake production.

By building up and providing access to a quality checked news data set for the relevant operational information space, the Rumour Debunker platform shows news, marked with the value of the compound index. As such, the news can be valued according to their reliability.

It is very easy to overlook whole parts of the internet communication, relevant for a specific crisis if these are manmade. Such traditional media monitoring methods do not have a proper grade of saturation for strategic communication. Automated methods have proven to be much more effective. However, most effective is the combination of automated tools and human intelligence, which is applied in Rumour Debunker.

Rumour Debunker platform shows news, marked with the value of the compound index. As such, the news can be valued according to their reliability.

Based on the data set of such classified news messages, users of the Rumour Debunker platform get an insight and impression on whether news are target of a hyper-personalised disinformation campaign. This possibility is expected to become more important for crisis and disaster management (CDM). So, in the future user might even be warned (if necessary) within the continuous media monitoring.

## UC2: Media observation in a crisis

For network centric communication in crisis and disaster management (CDM) it is very important to gather reliable open source information. Relevant sources of misinformation and disinformation must quickly be identified to react efficiently.

Social media is a facilitator/distributor of very sensitive public reactions. Changed communication rules in new media create new realities in possible and actual crisis situations. Traditional journalists lost their role as a gateway in crisis communication. With social media in place, crisis communication is always network centric. It needs crisis and disaster manager to use communication tools which keep up with the pace of innovation.

So, the first publisher might have a specific interest for publishing the information. The publisher with the highest multiplication rate is responsible for spreading the disinformation. For strategic network communication in crisis situations, it is very important to know the motivation behind disinformation campaigns, as well as first source and multiplication sources, so that they can be addressed appropriately and effectively.

In use case 2, by tracking the sources of specific news, back to their origin, the structure behind the disinformation campaign becomes visible.

### Test scenario corresponding to the use cases

#### TS #1 – Media Monitoring

Related use case: UC#1

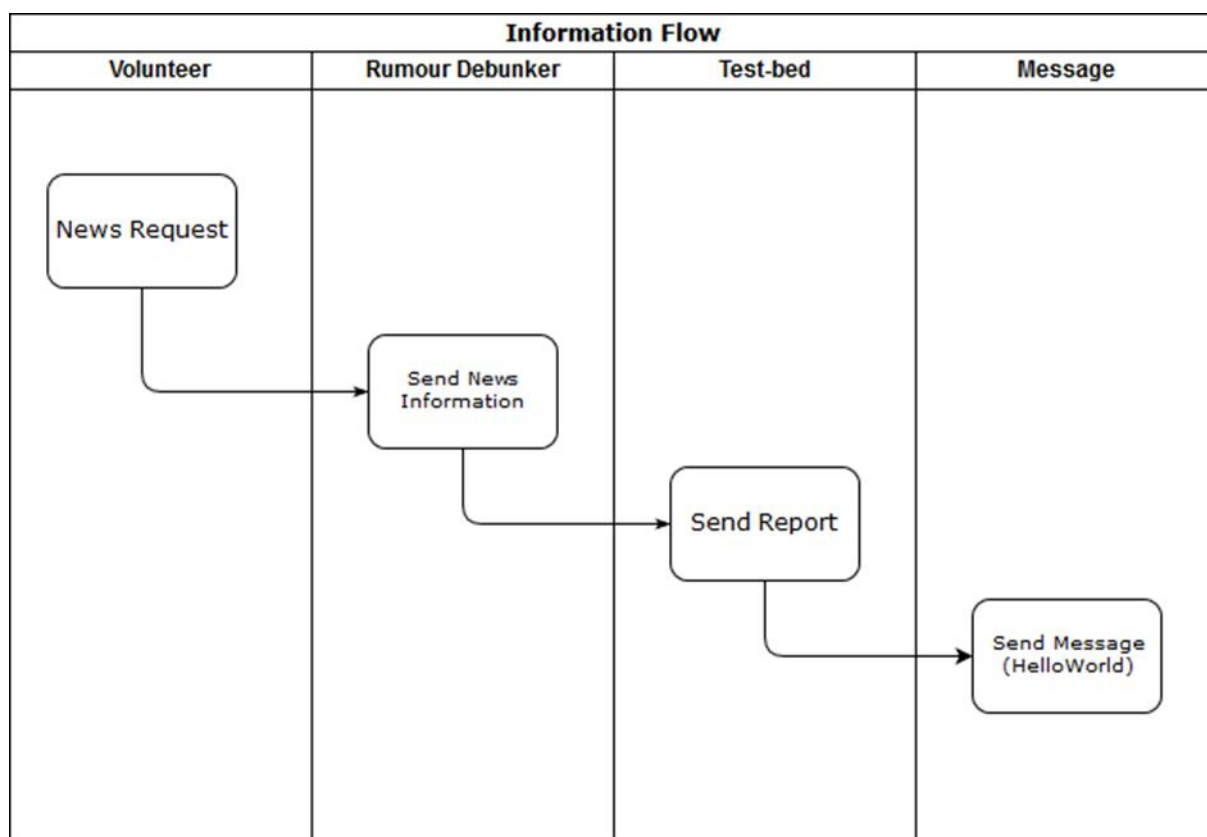


Figure 6.1: Information Flow in the Rumour Debunker solution integration scenario



### Description and objective:

The objective of UC1 is to provide continuous media monitoring, which can be achieved by the following steps:

1. The user requests a News update (either via the mobile app or the homepage <http://sf3.ait.ac.at/news>).
2. This request gets sent to the Rumour Debunker, which then starts a new update and processes the data into a Test-bed suitable format so that the information can then be sent to the Test-bed (via the JavaScript plugin).
3. The data gets sent to the Test-bed.
4. After the data has been processed in the Test-bed, the message “Hello World” gets displayed.

The test report of the Rumour Debunker solution integration is available in Annex 5.1.

### 6.3.2 Protect

Protect is a solution provided by DRIVER+ partner Edisoft. A description of the Protect solution can be found here: <https://pos.driver-project.eu/en/PoS/solution/59>.

Protect uses the REST adapter to connect to the Test-bed

The following back-end adaptations have been performed on the Edisoft Software/Middleware Framework for the Test-bed integration:

- Creation of a Virtual Machine.
- Installation of the Docker Engine.
- Installation of the Test-bed and Kafka in a container using a Docker Engine.

Adaptation of the existing mapping for incoming EMSI messages in Protect from external files:

- Development of a Rest adapter Endpoint in Protect.
- Subscribe the Test-bed Rest adapter with the Protect Endpoint.

The testing process of the Test-bed integration:

- Send an EMSI message successfully to the Test-bed Rest adapter (as an external entity).
- Receive the message using the Protect Endpoint Adopter.
- Send a message from Protect to the Test-bed Rest adapter.

All the tests were successful with a simple “Hello World” EMSI message. So, the proof of concept and the Test Bed are working properly with Protect.

However, Edisofts developer team detected that using Protect there were some EMSI messages that did not work properly, due to a problem in the Test Bed Rest adapter.

Frequentis was informed and solved an existing bug in the EMSI converter from XML to AVRO due to some ext. lib updates.

Frequentis turned available a new version of the Test Bed Rest adapter. Edisoft did the down load and installed the new version. This new version was tested and works properly and allows sending and receiving EMSI messages from Protect and the Test Bed. The following use cases have been defined for the integration of this solution with the Test-bed.

The test report of the Protect integration in form of screen shots is available in Annex 5.2.



### 6.3.3 IO-DA

A description of the IO-DA solution can be found here: <https://pos.driver-project.eu/en/PoS/solution/23>. The following use cases have been defined for the integration of this solution with the Test-bed.

#### 6.3.3.1 Description of IO-DA's UCs

##### UC – Get situation overview

As a user (member of the Crisis Management cell), I want to be able to get an overview of the crisis, of the critical infrastructures, the people able to help, and the potential risks. I would like to get a map of the crisis area, presenting the infrastructures of the area, and the risk/dangers of the area.

##### UC – Get decision help

As a user, member of the Crisis Management cell, I want to get help to decide how to solve the crisis. The outcome of the solution could be a process (BPMN) with all the actions that stakeholders must perform and in what order, in order to solve the crisis. I want this process to present the best and most efficient way out of the crisis, considering what are the stakeholders involved in the crisis solving process, their capacities, the infrastructures in the crisis area, and the context of the crisis.

#### 6.3.3.2 Selection of related solution

It was decided to integrate IO-DA with the solution LifeX Cop from Frequentis.

Since LifeX Cop can provide a map presenting the dangers and alerts of a crisis area, it was decided to connect with this solution and use the information about dangers and alert to complete the knowledge database of IO-DA. This will allow IO-DA to provide a process on how to solve the crisis.

#### 6.3.3.3 Description of a UC for the pair IO-DA and LifeX COP

##### UC#1 – Get a complete situation overview of the crisis, with the context, stakeholders, and objectives

IO-DA has a knowledge database composed of information about the context (geographic area) and the partners (stakeholders). This knowledge does not depend on any crisis; it is knowledge true at any time. Regarding a given area, the geographical context is always known (what are the landscape, the infrastructures, are there schools, hospitals, roads, etc. in the area?). It is also always known who the people are able to intervene in the area (firemen able to deal with fires, policemen able to set up a security area, emergency services are able to deal with the wounded, etc.). When a crisis occurs in the area, IO-DA needs to know what the objectives of this crisis are. I want solution B to send IO-DA the objectives of the crisis (georeferenced alerts about the crisis, where and when, category, urgency, etc. when it happens. This will allow completing the knowledge database of IO-DA. IO-DA can provide a GIS in order for the crisis cell to be able to visualise the different components of the crisis.

##### UC#2 – Get decision help

From the knowledge data base, completed thanks to the information sent by solution B, IO-DA will be able to provide a process in BPMN describing the theoretical best way to solve the crisis. This process will present all the actions to perform by the stakeholders as well as the order in which they have to perform them. This process is modifiable, which allows the user to change it if need be. Having this process will allow me to know how to best solve the crisis and will help me take efficient decisions.

The test scenario description and test report of the IO-DA solution integration is available in Annex 5.3.

### 6.3.4 EMT (Emergency Map Tool)

EMT Emergency Maps Tool is a solution provided by the AIT. A description can be found here: <https://pos.driver-project.eu/en/PoS/solution/26>.

For the integration of the EMT to the DRIVER+ Test-bed the Python Test-bed adapter from the DRIVER+ Github was used.

Back-end adaptations for the Test-bed integration:

- Download and installation of the DRIVER+ python-Test-bed-adapter, which enables connecting to the Test-bed and sending of an example message.
- Implementing CAP message, EMSI message and GeoJSON message handler for Test-bed consumer.
- Translating incoming messages to the EMT specific format.
- Implementation of a polygon compression for the incoming location data.
- Adaptation of the existing REST interface for the connection to the EMT.
- Setting up new EMT instance.
- Conversion of EMT format to EMSI, CAP and GeoJSON for Test-bed producer.

Front-End adaptations for the Test-bed integration:

- Configuration of the data message box layout in EMT for DRIVER+ Project.
- Configure new map layer for DRIVER+ messages.

Testing the integration:

- Starting of the Test-bed adapter consumer and producer, for sending and receiving messages via the Test-bed.
- Sending a generic CAP / EMSI message as a “Hello World” Example to the Test-bed via the producer.
- Receiving the “Hello World” message via the Test-bed consumer.
- Including location data to message.
- Including pictures with location tag to message.
- Creating CrowdTasker request in EMT and sending it via Test-bed producer to the CrowdTasker.
- Receiving Report from CrowdTasker via Test-bed consumer.
- Correctly displaying the received Report on the EMT map and the data table.

### 6.3.5 PROCeed Laboratory

A description of the PROCeed Laboratory solution can be found here: <https://pos.driver-project.eu/en/PoS/solution/68>). The following use case has been defined for the integration of this solution with the Test-bed.

**UC #1 – Provide possible future situational picture (objects attributes) to common operation picture tool:**

“As a COP or an operator, I want to receive information on possible future situational picture being a product of cascade effects predicted by PROCeed Laboratory tool, so that I can share this picture as a basis for making current decisions in the command centre.”

PROCeed Laboratory expects the following data:

- Background maps.
- Set and configuration of objects (protected assets, command posts, rescue units and vehicles, safeguards, etc.).
- Interdependencies among objects.

- Possibly user's assumptions/conditions.

Basing on the formerly introduced data, PROCeed simulates a chain of cascade effects to derive a Possible Future Situational Picture (PFSP). The resulting data may be useful for commanders in the decision-making process. Because decision makers use COP tool to observe the situation on the map acquired PFSP may be exported to the Test-bed to be imported by COP tool for visualisation. The PFSP consists of all objects in the given scenario with their geographical location and the rest of attributes (e.g. name, ownership, capacity, status, etc.). These data are put in the XML schema compliant with ETSI standard. Then they are sent to the Test-bed broker which stores them in an assigned topic for other applications. An import part to COP tool is still a subject of future development.

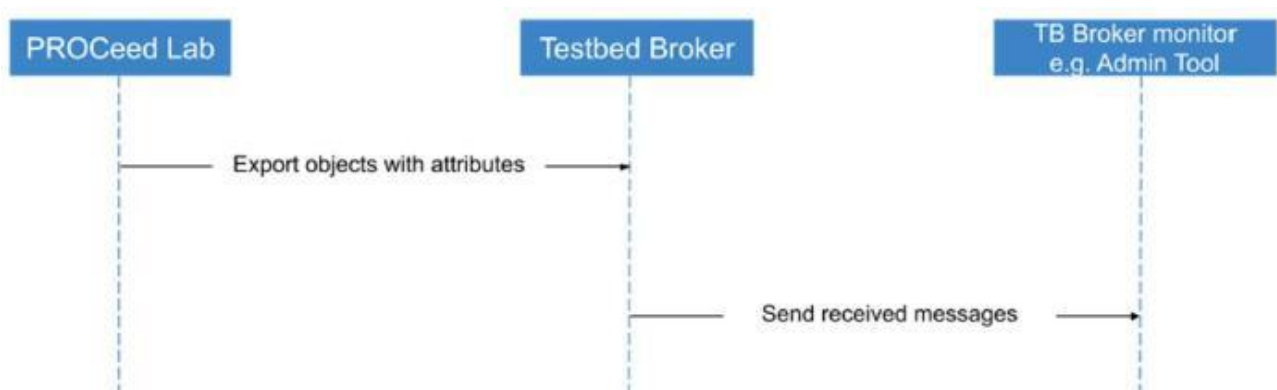
The following Test Scenario was executed related to the above UC#1:

### TS #1 – Distribution of objects attributes

The objective of UC#1 is to export PFSP to the Test-bed broker for other applications to use it (specifically by the COP tool). The ultimate goal of the process is to enhance the situational awareness of crisis managers by providing them possible courses of actions in the chain of cascade effects. Since the import to COP tool is still to be implemented it will be out of scope of this test case. The acceptance of the test case will be reached if the Test-bed broker receives exported messages. To prove it the Test-bed broker monitor (only for testing purpose) will be set up which will listen to the appropriate topic and will display all messages received. The following steps shall be taken to test the technological functionality that supports UC#1:

1. The PROCeed Laboratory operator logs into PROCeed Laboratory application and selects an exemplary scenario. Optionally, after this operation a typical simulation activity may be done in the application.
2. The PROCeed Laboratory operator clicks on the "EXPORT" button and activates the export method which exports all objects data of the selected scenario. PFSP is being sent to the Test-bed broker to specified topic using Test-bed adapter.
3. A tester verifies the messages received by the Test-bed broker using the Test-bed broker monitor checking if they have a correct syntax and if the information is compliant with the objects' configuration in PROCeed Laboratory.

A summary of the information flows generated as a part of these steps is shown in Figure 6.2.



**Figure 6.2: Sequence of information flow when visualising possible future situation (objects configuration)**

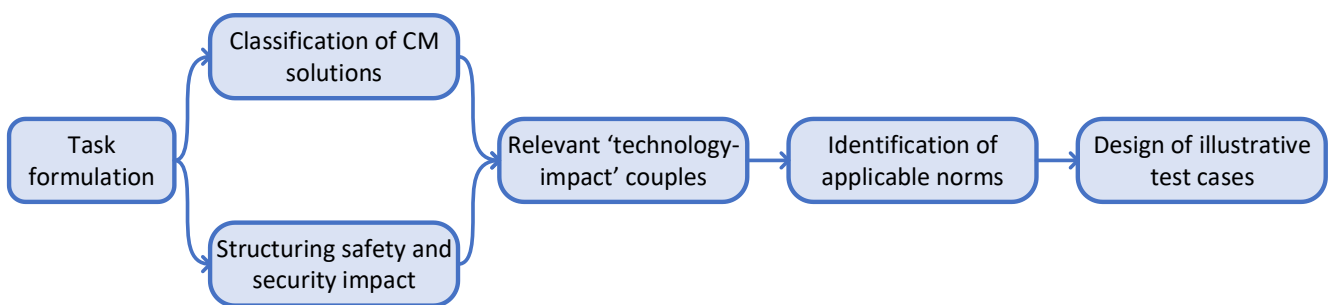
The test report of the PROCeed solution integration is available in Annex 5.4.

## 7. Considerations for future test and integration activities of Crisis Management solutions

### 7.1 Objectives and methodological approach

Crisis Management solutions trialled in the DRIVER+ project aim to fill-in identified Crisis Management gaps or increase the effectiveness or the efficiency in performing Crisis Management operations in a resource-constraint framework. Solution providers, often developing innovative ideas or exploiting emerging technological opportunities, aim to demonstrate new effects or more efficient use of limited Crisis Management resources in a realistic Trial setting. Less attention at this stage has been paid to additional considerations that might influence the wider use of a solution in an actual Crisis Management context.

This section of the report elaborates such additional considerations, namely the provision of safe and secure use of solutions in a real Crisis Management environment. The approach outlined on Figure 7.1 was followed.



**Figure 7.1: Safety and security related testing of Crisis Management solutions: Methodological approach.**

The task is to assist practitioners and solution providers in defining safety and security related requirements to Crisis Management solutions of interest and demonstrate how to develop respective test cases. Towards that purpose this section of the report provides:

- A classification scheme used to classify Crisis Management solutions on the basis of the underlying technology used.
- Structure of the safety and security considerations, i.e. the type of negative impact a solution may have.
- Identification of couples “technology – type of impact” where one has, or can realistically expect, concerns for the safe and secure use of a Crisis Management solution.
- Identification of applicable norms (standards, directives, regulations, etc.) for each “technology – type of impact” couple (presented in Annex 6 of this report).
- Design of illustrative test cases.

Each of the enumerated issues is examined in a sub-section below. The final sub-section outlines the envisioned implementation and future use of this approach to the safety and security related testing of Crisis Management solutions.

This approach was developed by the CSDM team in the DRIVER+ Consortium. In its draft form it was presented at DRIVER+ **SP93** meeting in Velizy, France, 13-14/05/2019. This section of the report presents an amended and refined version, resulting from the discussions in Velizy. The illustrative cases were developed by the TCS team.

## 7.2 Technology-based classification of solutions

---

To categorise Crisis Management solutions in terms of the underlying technology and in view of their potential impact on safety and security, three main taxonomies were analysed:

- STACCATO security taxonomy (STACCATO project, 2007) (16).
- CRISP Taxonomy of Security Products, Systems and Services (Sveinsdottir, 2014) (17).
- EDA Technology Taxonomy (European Defence Agency, no date) (18).

Furthermore a classification scheme with nine main categories was developed:

### 1. Sensors and navigation systems and networks

Passive (optical, IR, magnetic, acoustic, UW, electrical and electro-chemical sensors, magnetometers and magnetic gradiometers, gravity meters and gravity gradiometers) and active sensors (radar, ladar, lidar, sonars, X-ray, Gamma sensors, active IR sensors), chemical and biological substances detectors, radiological and nuclear detectors, etc.

### 2. Communications

Radio communications and networks; cable communications and networks; mass emergency notification systems; early warning and alerting systems; targeted emergency notification systems; secured, wireless broadband systems; rapidly deployable communication system (rescue services mobile communication system); emergency information hotlines.

### 3. Computer-based systems

Data bases and database management systems; decision support systems; training, modelling & simulation systems and environments; etc.

### 4. Specialised software applications

Personnel management software; material reserves management software; supply chain management software, information management & dissemination software; privacy and data protection software; electronic tagging systems; volunteers registries and management software, crowd sourcing/ crowd tasking systems.

### 5. Transportation vehicles and equipment

Ground, air, river, and maritime vehicles, ambulances, transportation containers and structures, etc.

### 6. Remotely controlled systems and autonomous vehicles and systems

RPVs/RPAS, air, ground, surface, sub-surface vehicles.

### 7. Fire extinguishers and decontamination devices and substances

Fire retardants, decontamination devices and substances for radiation sources, biological materials, chemical sources and poisons; etc.

### 8. Specialised disaster management equipment

Protective clothing and equipment, (mobile) shelters, mobile livestock shelters, mobile field hospitals, mobile energy systems and electricity generators, mobile water purification equipment, access control and

electronic authentication systems, training ranges, physical obstacles (e.g. to stop flooding), waste management systems, logistics tracking, transportation management systems, etc.

## 9. Training and personnel services

Education and skills training systems; psycho-social support systems; exercises; manuals; distance learning (e-Learning, m-Learning); fatigue and stress observation, analysis and coping system.

## 7.3 Types of potential safety and security impact of CM solutions

---

The implementation of Crisis Management solutions is expected to contribute to reduction of risks and more effective and efficient operations. However, they may have potential undesired side effects on the safety and security of personnel, property, infrastructure and the environment.

International Safety Standards define “safety” as freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment. Standards IEC 61508 and IEC 61511-1:2016 refer to this also as “functional safety.” In the discussion of Crisis Management solutions, the analysis of security concerns can start from the definition utilised by the International Society of Automation (ISA), i.e. “security” means prevention and protection from illegal or unwanted penetration, interference with proper operation or inappropriate access to confidential information regardless of motivation (intentional or unintentional) or consequence (result).

Starting from these definitions, and accounting for societal and environmental concerns, this study examines the potential negative impact of Crisis Management solutions on:

- People, both those involved in Crisis Management and others who happen to be at or near the crisis scene.
- The equipment and/or the data and information used in Crisis Management.
- The functioning of critical infrastructures, e.g. energy, transport (EU Council, 2008 (19)), digital infrastructure) and the delivery of essential services, e.g. food, water, financial services (EU Council, 2016), etc.
- The environment, i.e. on the animals, the vegetation, air, soil, and water quality.

Respectively, here only direct impact is considered, not taking into account possible cascading effects, e.g. software breach leading to a drone crash and injury of first responders. The reason is that testing will be conducted to assure that a Crisis Management solution meets the requirements of certain safety and security norms, while potential secondary effects may be studied via more complex models or Trial scenarios.

Hence, seven types of negative impact, marked from A to G, are taken into consideration:

Impact on humans (professional responders and other Crisis Management personnel, volunteers, service providers, other people in the area of the crisis or its vicinity):

- A. Physical (injury, poisoning, blinding, death, etc.).
- B. Psychological impact; impact on the perceptions.
- C. Breach of sensitive personal data.

Temporary or lasting impact on Crisis Management materiel, data, and information (equipment, communications, information, etc.):

- D. Obstructing the use of CM equipment (e.g. by physical damage, radio-electronic interference, etc.).
- E. “CIA” – impact on the confidentiality, integrity and availability of information (including malicious attempts to manipulate information).

- F. Impact on critical infrastructures and/or the provision of essential services.
- G. Environmental impact (flora, fauna, soil, air, water).

## 7.4 Pertinent “Technology-Impact” combinations

---

There are 63 possible combinations among the nine categories of solutions and the seven types of impact (see Table 7.1). Not all combinations are possible, i.e. certain categories of solutions cannot have a particular type of impact (only direct impact is considered here; possible cascading effects are not subject of this study). For example, a software application is highly unlikely to cause physical injury, transportation vehicles and decontamination devices are unlikely to infringe on the confidentiality, integrity and availability of information, etc.

In Table 7.1, the cells of such unlikely combinations are marked with grey background colour. The remaining 39 combinations “solution’s underlying technology – negative impact on safety and security” are considered pertinent. Respectively, Annex 6 provides standards and other norms for each pertinent combination, while Annex 7 provides illustrative test cases for the “Technology-Impact” combinations marked with “X” in Table 7.1.



Table 7.1: Technology-Impact of combinations.

Potential impact on/	Humans			CM materiel, data, and information			
Solutions	A. Physical	B. Psychological, perceptions	C. Personal data	D. Materiel	E. CIA of information	F. Critical infrastructures	G. Environment
<b>1. Sensors and navigation systems and networks:</b> passive (optical, IR, magnetic, acoustic, UW, electrical and electro-chemical sensors, magnetometers and magnetic gradiometers, gravity meters and gravity gradiometers) and active sensors (radar, ladar, lidar, sonars, X-ray, Gamma sensors, active IR sensors), chemical and biological substances detectors, radiological and nuclear detectors, etc.							
<b>2. Communications:</b> Radio communications and networks; cable communications and networks; mass emergency notification systems; early warning and alerting systems; targeted emergency notification systems; secured, wireless broadband systems; rapidly deployable communication system (rescue services mobile communication system); emergency information hotlines.							
<b>3. Computer-based systems:</b> data bases and database management systems; decision support systems; training, modelling & simulation systems and environments; etc.						X	
<b>4. Specialised software applications:</b> Personnel management software; material reserves management software; supply chain management software, information management and dissemination software; privacy and data protection software; electronic tagging systems; volunteers registries and management software, crowd sourcing/ crowd tasking systems.			X		X		
<b>5. Transportation vehicles and equipment:</b> ground, air, river, and maritime vehicles, ambulances, transportation containers and structures, etc.							
<b>6. Remotely controlled systems and autonomous vehicles and systems:</b> RPVs/RPAS, air, ground, surface, sub-surface vehicles.							
<b>7. Fire extinguishers and decontamination devices and substances:</b> Fire retardants, decontamination devices and substances for radiation sources, biological materials, chemical sources and poisons.							
<b>8. Specialised disaster management equipment:</b> protective clothing and equipment, (mobile) shelters, mobile livestock shelters, mobile field hospitals, mobile energy systems and electricity generators, mobile water purification equipment, access control and electronic authentication systems, training ranges, physical obstacles (e.g. to stop flooding), waste management systems, logistics tracking, transportation management systems, etc.							
<b>9. Training and personnel services:</b> Education and skills training systems; Psycho-social support systems; Exercises; Manuals; Distance learning (e-Learning, m-Learning); Fatigue and stress observation, analysis and coping system.							

## 7.5 Sample safety and security norms for pertinent “Technology-Impact” combinations

---

Selected regulations on safety and security of Crisis Management solutions are presented in Annex 6.

## 7.6 Illustrative test cases

---

Annex 7 outlines three illustrative test cases for testing safety and security of Crisis Management solutions that have already participated in project Trials:

- The Social Media Analysis Platform, trialled in Trial France.
- The CrisisSuite solution, trialled in Trials France and The Netherlands, and in the Final Demo.
- The Test-bed infrastructure with the Common Information Space and its embedded security features.

The role and the guidelines for preparing test cases are described in DRIVER+ deliverable **D934.21 – Solution Testing Procedure** (6).

## 7.7 Implementation

---

Assuring safety and security of new Crisis Management solutions depends on the way practitioners’ organisations define their requirements. Solution providers or third parties are expected to warrant that these requirements are met. It is possible also to jointly design and conduct tests to verify the extent to which requirements are met.

This section of the report is intended to support the process by presenting a framework for dealing with safety and security concerns in the use of Crisis Management solutions in actual crisis context, which would be of use to both Crisis Management practitioners and solution providers.

While this framework is comprehensive, the list of normative documents (Annex 6, announced in sub-section 7.5) is subject to continuous review, updates and amendment. This also applies to illustrative test cases, presented in sub-section 7.6 and Annex 7. An increasing number of test cases and results will contribute to the body of knowledge on the safe and secure use of solutions in actual Crisis Management context.

## 8. Conclusions

---

The overall goal of the solution integration is that crisis relevant information is presented to practitioners in the most suitable and comfortable way considering the challenges they face during their crisis response actions. An automated exchange of data among involved IT solutions shall avoid that practitioners face an information overload. The solution integration leads to an aggregation of subsystems which cooperate in an automated way so that the system of integrated solutions achieves an overarching functionality. It has to be mentioned that many solutions used in DRIVER+ Trials were prototypes and thus do not have the maturity level of a product. A direct comparison between the mature products currently used by practitioners and the new DRIVER+ solutions cannot be objective for this reason.

The document describes all work necessary to achieve this automated exchange of data between different IT solutions and Trial 3, 4 and the Final Demo made a tendency visible that the solution integration (once it will be performed in an operational environment with fully mature products) will lead to:

- Less time needed for practitioners in their search for crisis relevant information.
- More comfort for practitioners to find relevant information due to optimized presentation of information (e.g. by using user interfaces which are familiar to them).
- Less time needed for practitioners to read data from one solution and entering data manually into another solution.
- Lower probability for wrong information caused by human errors while reading/entering data from/into a solution.
- More time left for practitioners to analyse and interpret the information and to define, communicate, execute and supervise crisis response actions.
- Higher quality of the Crisis Management outcome due to time savings, better data quality and improvements in crisis relevant communication.

However, there are several lessons learned which result from the experience in the solution integration process and which reveal some aspects which need to be considered:

- The definition of a clear process and timeline for the whole solution integration process, from the creation of use-cases until the final tests to verify the integration is key and must be communicated to all involved parties.
- The use-cases need to be specified as exactly as possible - starting point shall always be the Use-cases from an end user perspective which will have to be translated into technical UML diagrams for the data exchange among the involved solutions, followed by test-cases how this interaction is verified.
- The concept of having at least two Dry-Runs before each Trial has proven to be necessary and valuable. The interaction between a scenario and the involved solutions requires those physical meetings (on top of telephone conferences and remote testing) where the major actors prepare the Trial and iteratively improve scenario details and technical integration details.
- The Dry-Runs did not always provide enough time to perform all tests at a timescale corresponding to the original Trial scenario. Some tests were shortened for this reason but did not produce the same behaviour of solutions as detected later at original scenario length. The ideal status that all solution providers achieve the same level of integration was often not achieved. One solution not being fully integrated often delayed the progress of the testing.
- As a first integration step solutions will need to be integrated into the data exchange platform (DRIVER+ test-bed) for basic data exchange capabilities. The technical capabilities of the solutions have to be analysed in order to select the appropriate Test-bed Adapters. Solutions need to be made ready for the integration either by configuration or by software updates to make them able to access the selected Test-bed Adapters. Test cases will have to be elaborated, aiming at verifying each step of the data exchange.
- A progressive increase of the number of solutions for the data exchange is useful as fault finding and bug fixing is easier if lower numbers of solutions are involved.

- Proper documentation of each step (e.g. for configuration and test setups) is key in order to support future test and bug fixing work.
- Planning with realistic timespans for each of the steps above is important, as not all steps will work smoothly from the beginning and some steps might have to be repeated.
- Even though the solution trainings were performed during Dry-Run 2 and again during the week of the Trials, they were often perceived to be too short by the practitioners, as not only the isolated solutions, but also the effects of the solution integration had to be explained. To profit from all the benefits a solution and the integration of solutions could offer, even more focus shall be put on the solution trainings and the embedment of the integrated solutions in their work processes, and correspondingly more time should be planned for.
- Remote testing became an important part of the preparation work for Trial 3, 4 and the Final Demo and proved to be very time and cost efficient. It requires proper planning of the corresponding setup at all involved parties.
- The implemented chat forums for technical discussions (Slack) proved to be valuable for the preparation of Trial 3, 4 and the Final Demo and a more structured technical knowledge exchange (compared to the usage of e-mails).

## References

---

1. **DRIVER+ project.** *D934.31 - DRIVER+ Solution scenarios and integration test results V1.* Nov. 2018.
2. —. *D922.11 - List of CM gaps.* 2018.
3. —. *D942.24 - Report on the application of solutions in Trial 3.* 2019.
4. —. *D942.23 - Report on the application of solutions in Trial 4.* 2019.
5. —. *D947.12 Report on Trial Evaluation - Final Demo.* 2020.
6. —. *D934.21 - Solution Testing Procedure.* 2018.
7. —. *D923.11 - Test-bed functional specification.* 2018.
8. —. *D923.21 - Report on the Test-bed reference implementation.* 2018.
9. —. *D923.23 - Final release of the Test-bed reference implementation.* 2019.
10. —. *D945.11 - Report on Trial Action Plan - Trial 3.* 2019.
11. —. *D946.11 - Report on Trial Action Plan - Trial 4.* 2019.
12. **OASIS.** Common Alerting Protocol Version 1.2. [Online] 2010.
13. **Internet Engineering Task Force (IETF).** *RFC 7946 - The GeoJSON Format.* 2016.
14. **The Open Source Geospatial Foundation (OSGeo).** *GeoTIFF.* 2018. <https://trac.osgeo.org/geotiff/>.
15. **DRIVER+ project.** *D932.12 - PoS Tutorial and Recommendations.* 2019.
16. **AeroSpace and Defence Industries Association of Europe.** *STACCATO Final Taxonomy, Deliverable 1.2.2, STACCATO (Stakeholders Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities) project.* 2007.
17. **Thordis Sveinsdottir et al.** *“Taxonomy of Security Products, Systems and Services”, Deliverable 1.2, CRISP (Project title: Evaluation and Certification Schemes for Security Products) project.* July 2014.
18. **European Defence Agency, n.d.** *EDA Technology Taxonomy Overview, available at <https://www.eda.europa.eu/docs/default-source/procurement/eda-technology-taxonomy.pdf>.*
19. **European Parliament and Council .** *Directive 2008/68/EC of the European Parliament and of the Council of 24 September 2008 on the inland transport of dangerous goods.* 2008.

20. **2016, European Parliament and the Council of 6 July.** *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, pp. 1–30, . s.l. :* <http://data.europa.eu/eli/dir/2016/1148/oj>, 19.17.2016.

## Annex 1 – DRIVER+ Terminology

In order to have a common understanding within the DRIVER+ project and beyond and to ensure the use of a common language in all project deliverables and communications, a terminology is developed by making reference to main sources, such as ISO standards and UNISDR. This terminology is presented online as part of the Portfolio of Solutions and it will be continuously reviewed and updated<sup>5</sup>. The terminology is applied throughout the documents produced by DRIVER+. Each deliverable includes an annex as provided hereunder, which holds an extract from the comprehensive terminology containing the relevant DRIVER+ terms for this respective document.

**Table A1: DRIVER+ Terminology**

Terminology	Definition	Source
<b>Crisis Management function</b>	Crisis Management functions aim at achieving effects, e.g. coordination, a direction of effort, shared awareness, etc., in a Crisis Management system-of-systems. The “function” focuses on what is to be achieved, not how or by whom. Several systems, tools, building blocks, etc. may individually or in concert deliver a given function and, conversely, may support several different functions. Crisis Management functions are grouped in three functional areas: operational (protection, response, recovery), preparatory (mitigation, capability development, strategic adaptiveness) and common (security management, logistics, C3, comms & Info management).	Initial DRIVER+ definition
<b>Dry Run 1</b>	First rehearsal of a Trial, focusing on the technical integration of solutions, reference implementation of the Test-bed, and scenario validation; it also serves as a readiness review to approve the maturity of technical solutions.	Initial DRIVER+ definition
<b>Dry Run 2</b>	Full scale rehearsal of a Trial without external practitioner participation, aimed at detection of technical issues and last second fine-tuning; Dry Run 2 is organized as a complete mirror of the Trial.	Initial DRIVER+ definition
<b>Gap</b>	Gaps between the existing capabilities of responders and what was actually needed for effective and timely response.	Project Responder 5
<b>Interoperability</b>	The ability of diverse systems and organisations to work together, i.e. to interoperate.	ISO 22397
<b>Legacy systems</b>	(Crisis Management) system currently in operational use.	Initial DRIVER+ definition

<sup>5</sup> The Portfolio of Solutions and the terminology of the DRIVER+ project are accessible on the DRIVER+ public website (<https://www.driver-project.eu/>). Further information can be received by contacting [coordination@projectdriver.eu](mailto:coordination@projectdriver.eu).



Terminology	Definition	Source
<b>Operator</b>	(Human) operator Person engaged in task performance, considered as a monitoring, controlling or directing element in a system or process capable of a dynamic response to system inputs and disturbances.	ISO 9996:1996(en) Mechanical vibration and shock — Disturbance to human activity and performance — Classification, 3.5
<b>Portfolio of Solutions (PoS)</b>	A database driven web site that documents the available Crisis Management solutions. The PoS includes information on the experiences with a solution (i.e. results and outcomes of Trials), the needs it addresses, the type of practitioner organisations that have used it, the regulatory conditions that apply, societal impact consideration, a glossary, and the design of the Trials.	Initial DRIVER+ definition
<b>Solution</b>	A solution is a means that contributes to a Crisis Management function. A solution is either one or more processes or one or more tools with related procedures.	Initial DRIVER+ definition
<b>Test-bed</b>	The software tools, middleware and methodology to systematically conduct Trials and evaluate solutions within an appropriate environment. An “appropriate environment” is a testing environment (life and/or virtual) where the trialling of solutions is carried out using a structured, all-encompassing and mutual learning approach. The Test-bed can enable existing facilities to connect and exchange data, providing a pan-European arena of virtually connected facilities and crisis labs where users, providers, researchers, policy makers and citizens jointly and iteratively can progress on new approaches or solutions to emerging needs.	Initial DRIVER+ definition

## Annex 2 – Trial 3 – Technical details

This annex provides some technical details related to the Trial 3.

### Data Exchange Diagram

Figure A2.1 provides an overview of which kind of data was exchanged between which solutions, using which Standards, in the scope of which test cases.

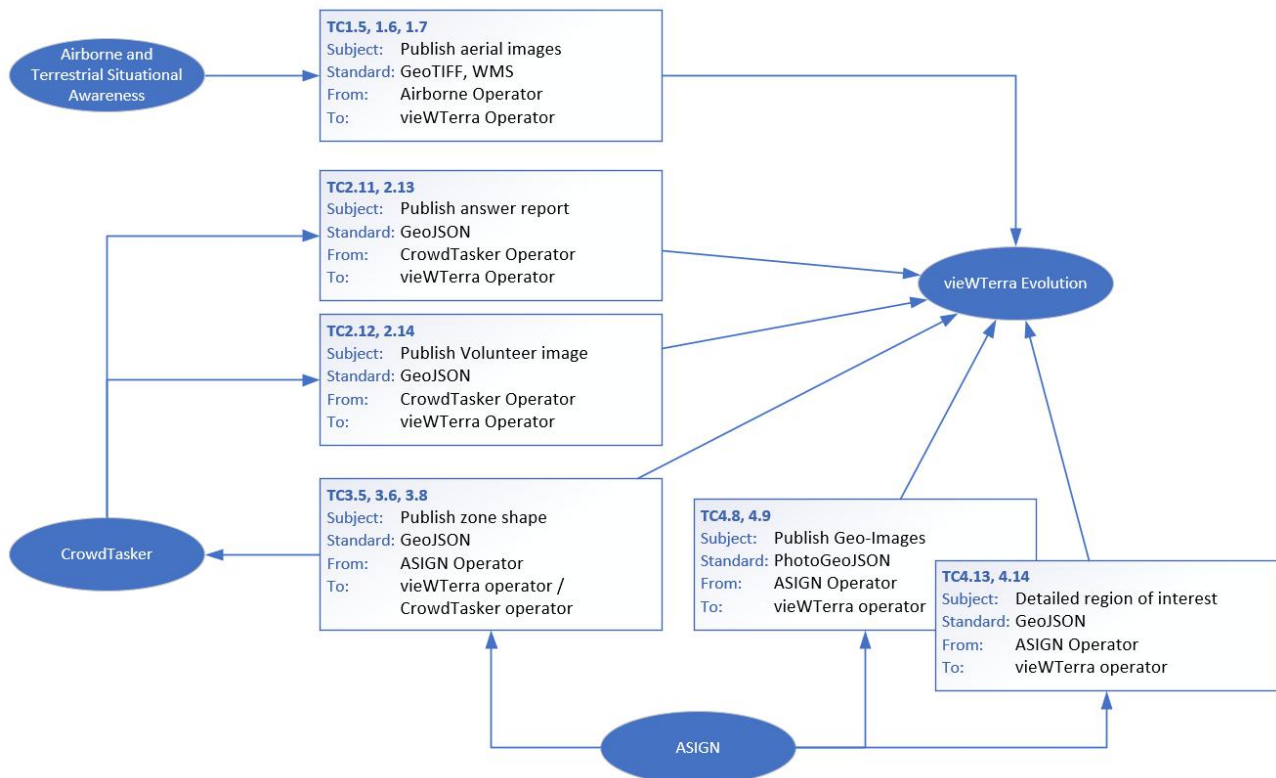
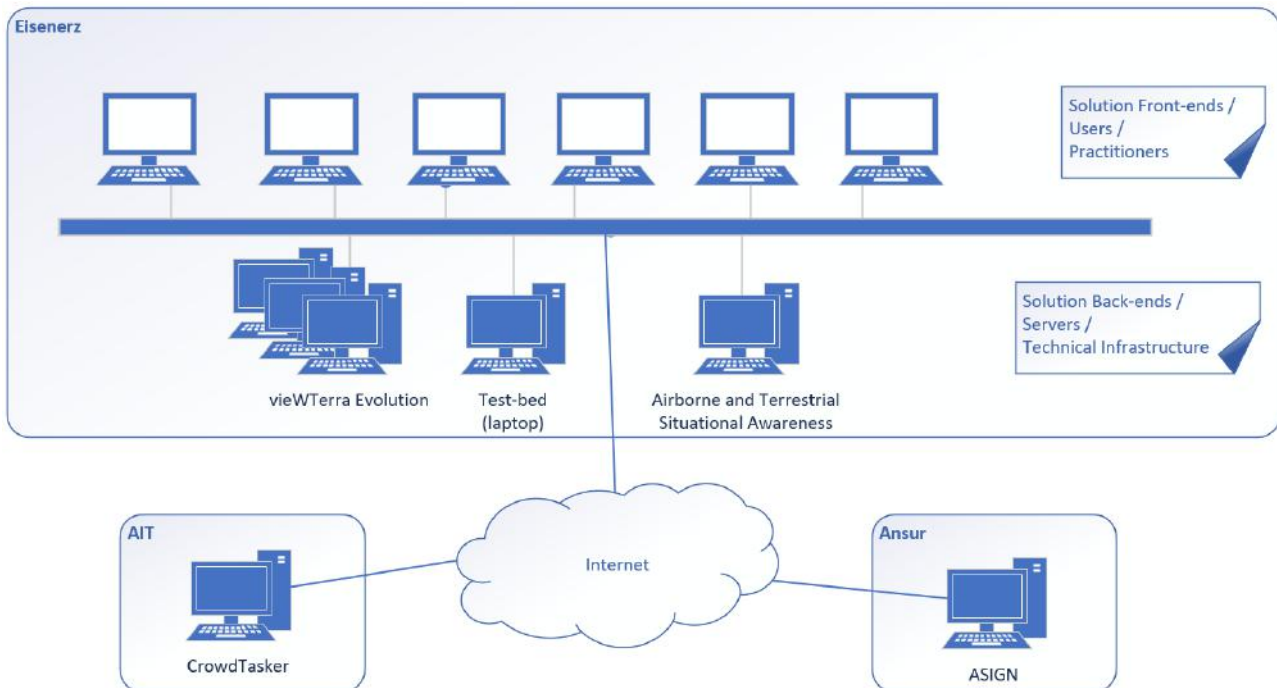


Figure A2.1: Data Exchange Diagram of Trial 3

### Solution and Test-bed deployment

The physical deployment of computers (clients and servers) used by solutions for Trial 3 is visualised in Figure A2.2. The back-ends (servers) for the solutions vieWTerra Evolution and Airborne and Terrestrial Situational Awareness as well as the Test-bed were all hosted at the command centre for Crisis Management in Eisenerz. The server for the CrowdTasker solution was remotely hosted by the Austrian Institute of Technology (AIT); the ASIGN server was remotely hosted by AnsuR.



**Figure A2.2: Physical deployment of solution back-ends for Trial 3**

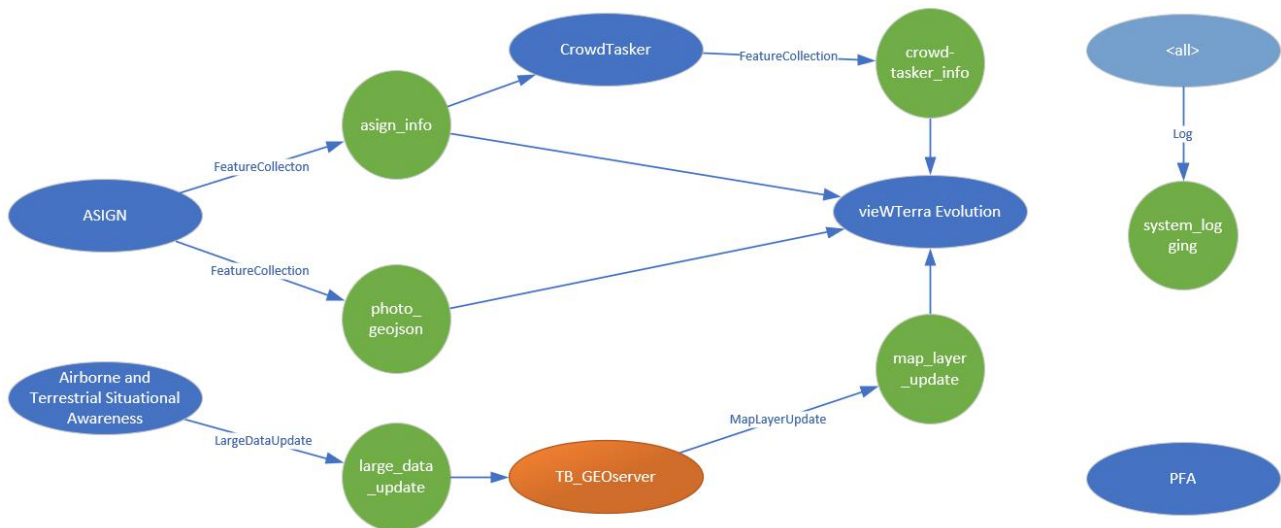
### Communication channels configured in the Test-bed

Figure A2.3 provides an overview of the technical integration of the solutions with the Test-bed. The green circles in this figure represent so-called “topics”, which are pre-configured in the Test-bed for Trial 3 to realise the communication channels between solutions. On one hand, each solution may publish messages of a certain type onto certain topics; on the other hand, each solution may subscribe at certain topics in order to receive all messages that are published on that topic. Just as an example: the ASIGN solution publishes “FeatureCollection” messages to the “photo\_geojson” topic as well as other “FeatureCollection” messages to the “assign\_info” topic. Solutions CrowdTasker and vieWTerra subscribe to the “assign\_info” topic – so they will receive the corresponding “FeatureCollection” messages from ASIGN solution.

Note that all solutions provide log messages to the “system\_log” topic.

Note that PFA as a non-technical solution is not using any topics and therefore appears as a standalone ellipse in the figure.

Note that TB\_GEOserver is a Test-bed component rather than a solution on its own.



**Figure A2.3: Technical solution integration, using various topics configured in the Test-bed**

As active Test-bed features the following topics have been used in Trial 3:

- Core topics
  - System\_heartbeat (all solutions sending out their “alive” status).
  - System\_admin\_heartbeat (the Admin Tool sending out its “alive” status).
  - System\_logging (logs for all solutions and Admin Tool).
  - System\_topic\_access\_invite (allowing solutions to listen to all standard topics).
  - System\_session\_mgmt (sent by TMT for Session Start/Stop).
  - System\_phase\_message (sent by TMT for new Phase information).
  - System\_role\_player\_message (sent by TMT indicating a Player needs to perform a manual action).
  - System observer\_tool\_answer (sent by OST to report Observer Answers).
- Standard topics (<https://github.com/DRIVER-EU/avro-schemas/tree/master/standard>):
  - large\_data\_update  
Large Data Update: [https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system\\_large\\_data\\_update-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system_large_data_update-value.avsc).
  - map\_layer\_update  
Map Layer Update: [https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system\\_map\\_layer\\_update-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system_map_layer_update-value.avsc).
  - photo\_geojson  
PhotoGeoJSON: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/photo-geojson/photo\\_geojson-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/photo-geojson/photo_geojson-value.avsc).
  - assign\_info  
GeoJSON: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard\\_geojson-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard_geojson-value.avsc).
  - crowd-tasker\_info  
GeoJSON: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard\\_geojson-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard_geojson-value.avsc).

### Solution Integration Sequence Diagrams

The figures below provide some example sequence diagrams that were created automatically out of the recordings produced by the After-Action Review tool during the execution of Trial 3 on 12-13/09/2019. The complete AAR recording is available online on <http://134.221.20.201:8199/#/>.



Figure A2.4: Trial 3 – Sub-scenario #2 sequence diagram – example extract

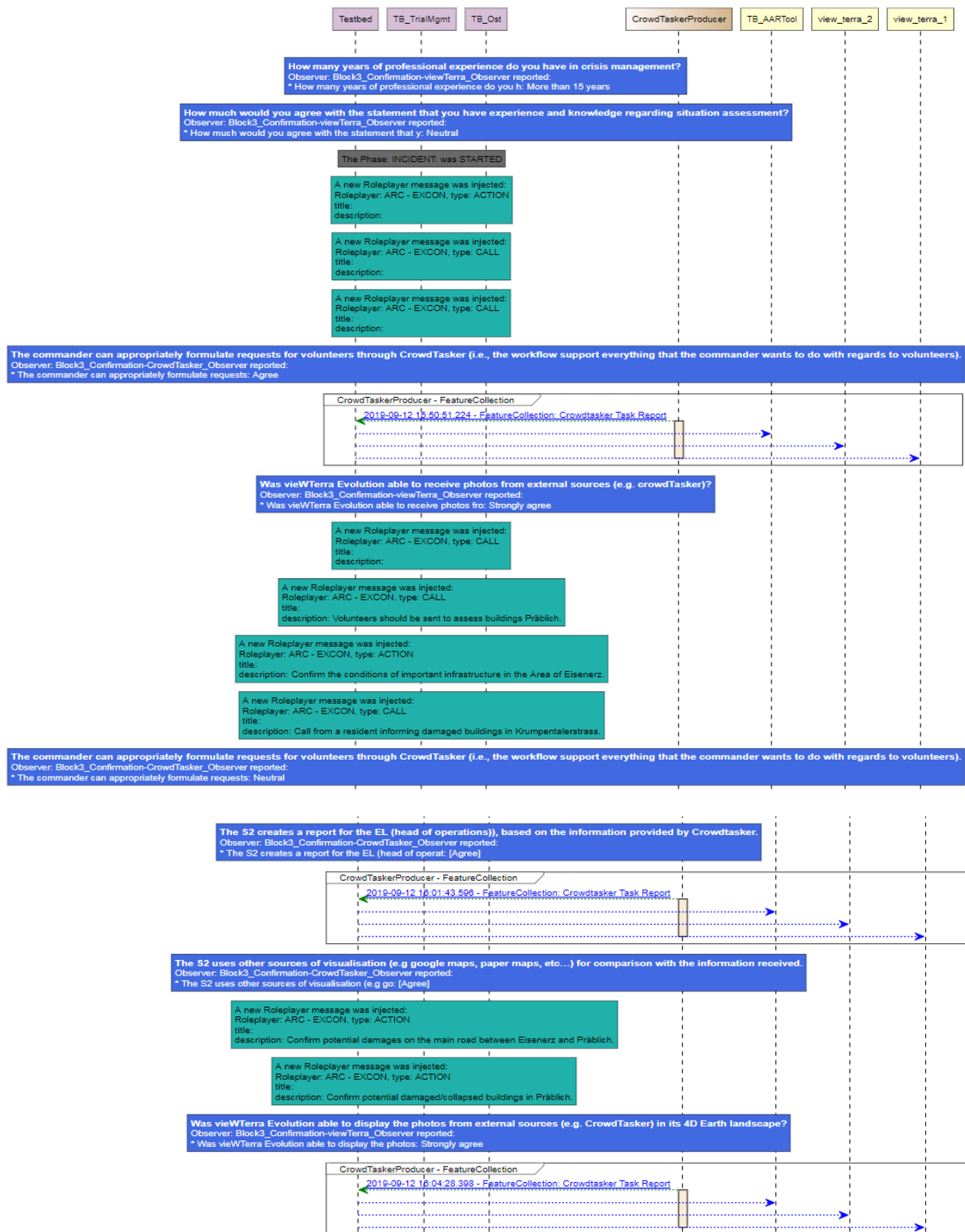


Figure A2.5: Trial 3 – Sub-scenario #3 sequence diagram – example extract

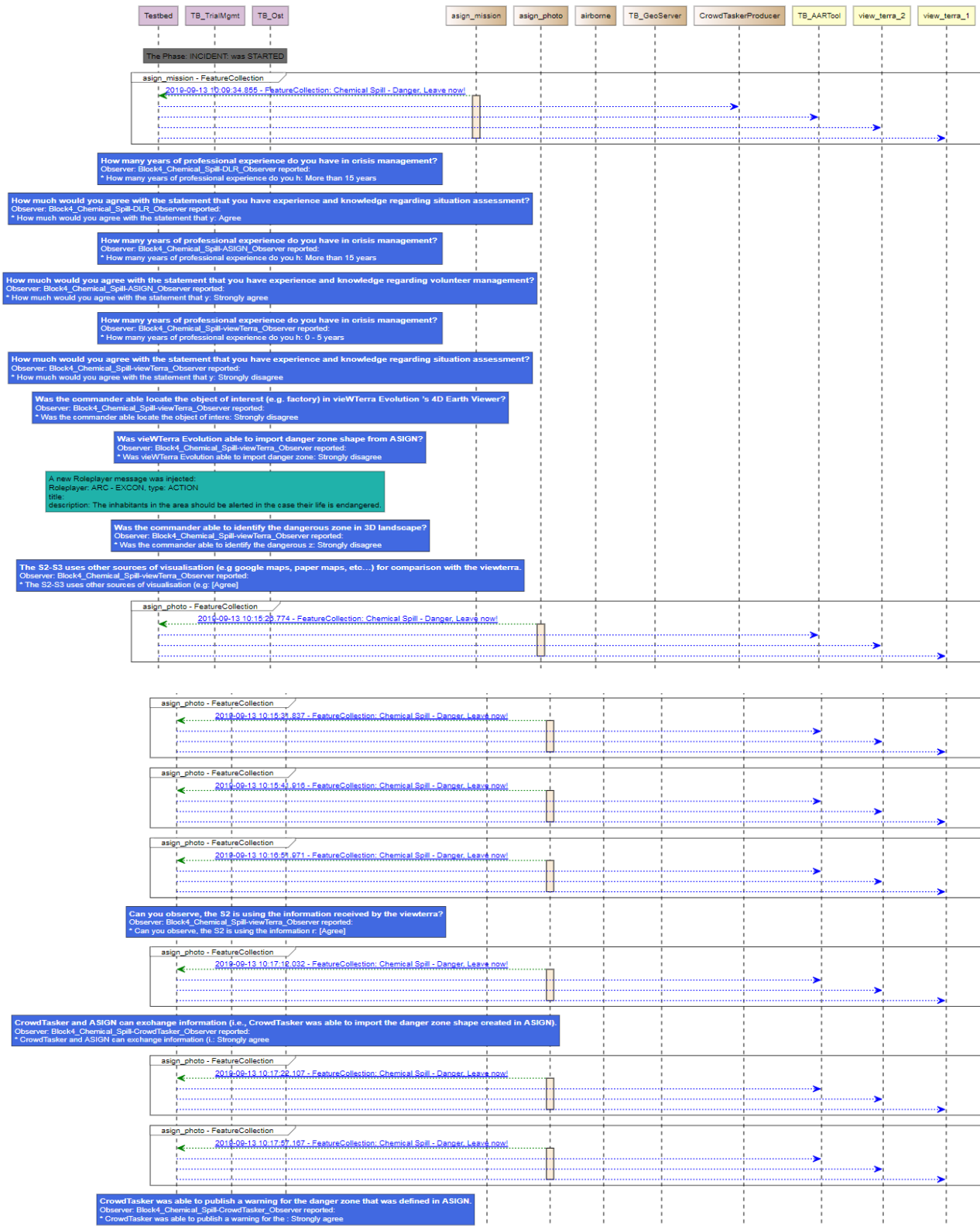


Figure A2.6: Trial 3 – Sub-scenario #4a sequence diagram – example extract



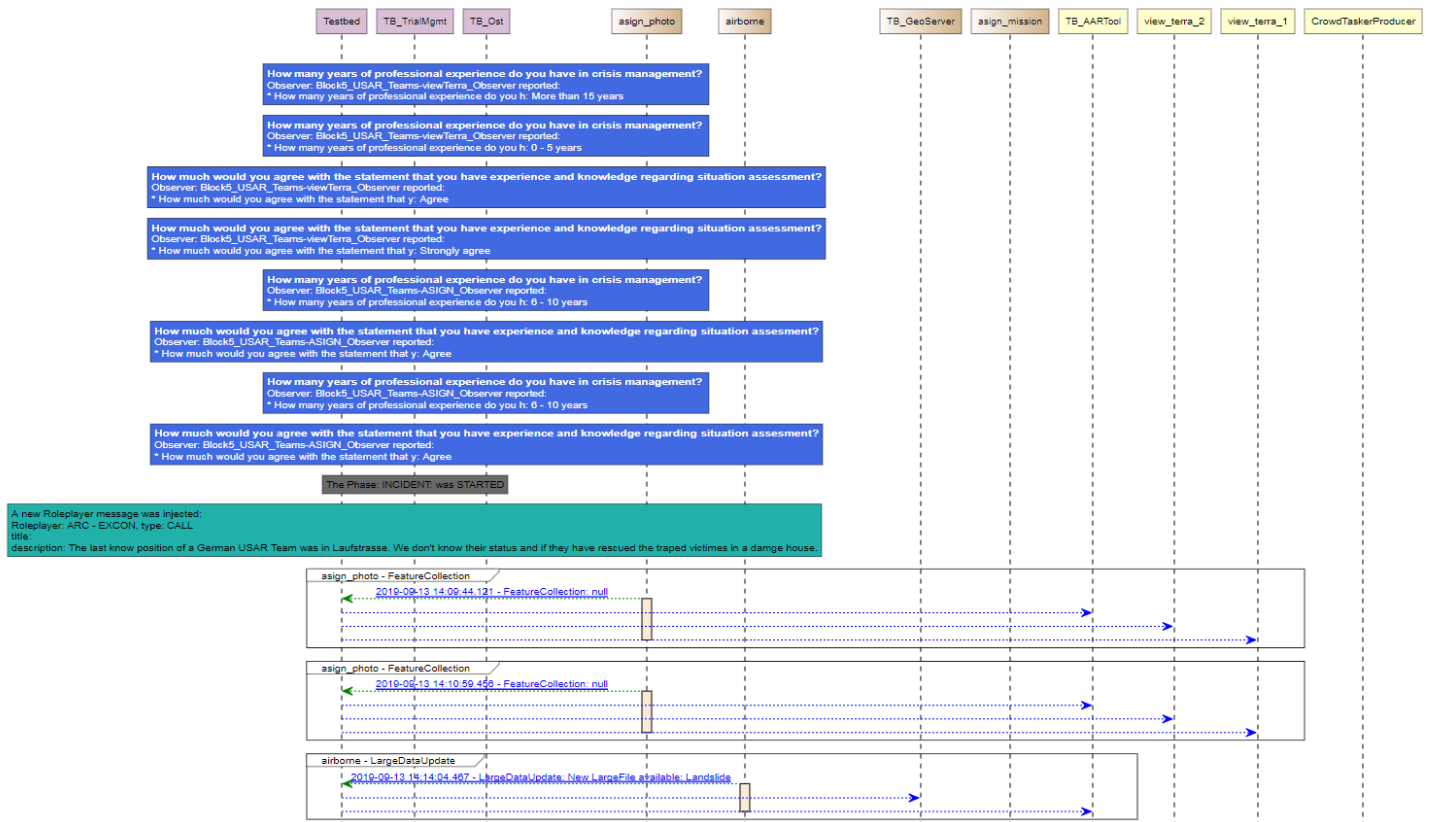


Figure A2.7: Trial 3 – Sub-scenario #5 sequence diagram – example extract

### Solution Integration – Test-bed messages

This section provides examples of messages as they were recorded by the After-Action Review tool during the execution of Trial 3 on 12-13/09/2019. All AAR recordings are available online on <http://134.221.20.201:8199/#/>.

Table A2.1: Trial 3 – LargeDataUpdate message example

LargeDataUpdate Message	
Sender	airborne
Topic	large_data_update
Message content	<p>Record ID: 2190</p> <p>Headline: New LargeFile available: Landslide</p> <p>URL: ftp://f_argos:Vabene01@plapperkaefer/ftp/mosaike/TrainAFTER_20190913_101237_15cm_495C</p> <p>Data Type: image_geotiff</p> <p>Title: Landslide</p> <p>Description: 47.538404,14.933562,47.524917,14.953506</p> <p>Attachments:</p>

Table A2.2: Trial 3 – FeatureCollection message example


FeatureCollection Message	
Sender	ASIGN
Topic	photo_geojson
Message content	<p>Record ID: 2314</p> <p>Map:</p>  <p>Headline: USAR Mission</p> <p>Client ID: assign_photo</p> <p>Date/Time: 2019-09-13 16:02:17.551</p> <p>Level:</p> <p>Attachments:</p>

Table A2.3: Trial 3 – MapLayerUpdate message example

MapLayerUpdate Message	
Sender	GeoServer
Topic	map_layer_update
Message content	<p>Record ID: 1380</p> <p>Headline: Flug2_20190911_095445_15cm_490! CREATE</p> <p>Client ID:</p> <p>Attachments:</p> <p>Message:</p> <pre> {   "url": "http://192.168.178.31:8180/geoserver/driver/wms",   "title": "Flug2_20190911_095445_15cm_490500_526650",   "description": "47.551851,14.873736,47.538374,14.893700",   "username": null,   "password": null,   "updateType": "CREATE",   "layerType": "WMS" } </pre>

## Annex 3 – Trial 4 – Technical details

This annex provides some technical details related to the Trial 4.

### Data Exchange Diagram

Figure A3.1 provides an overview of which kind of data was exchanged between which solutions, using which standards, in the scope of which test cases.

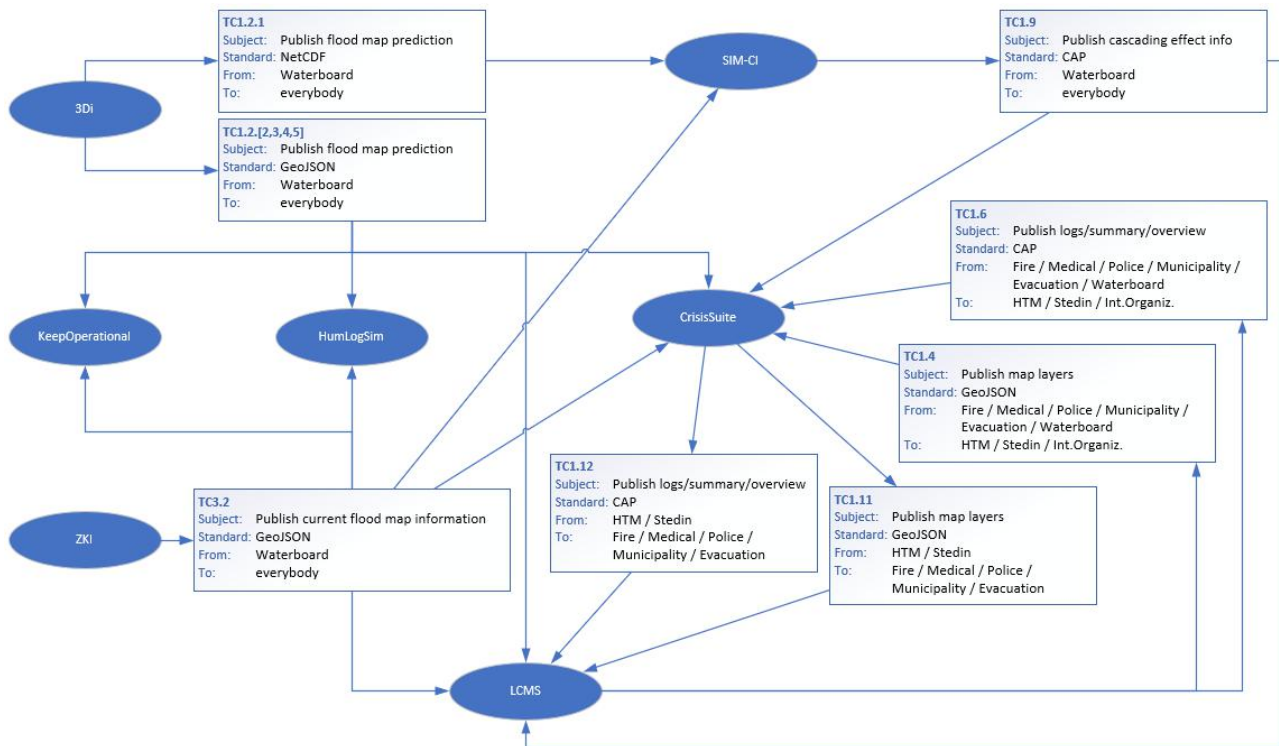
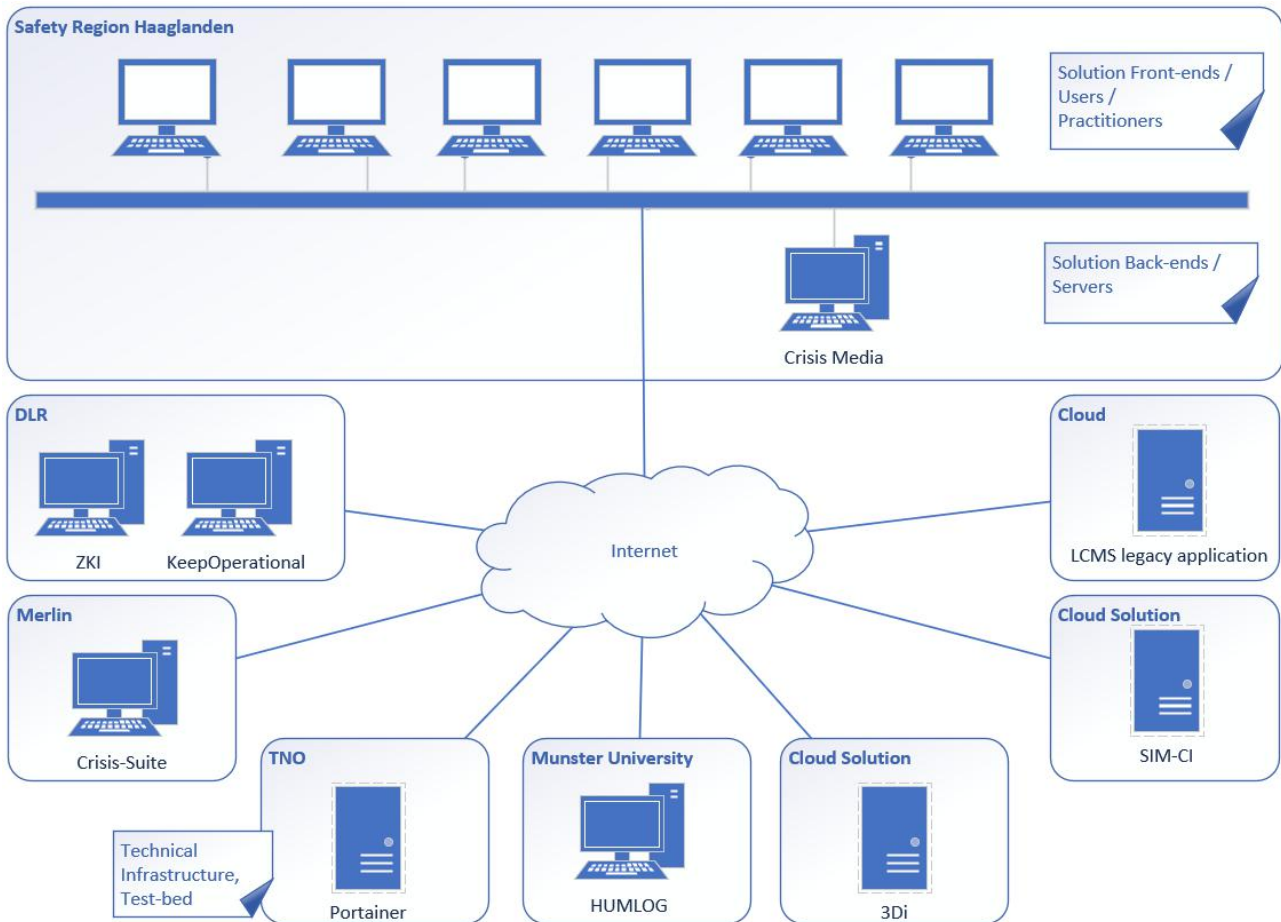


Figure A3.1: Data Exchange Diagram of Trial 4

### Solution and Test-bed deployment

The physical deployment of computers (clients and servers) used by solutions for Trial 4 is visualised in Figure A3.2. This figure illustrates that the technical integration of solutions for Trial 4 was highly distributed. The headquarters for Crisis Management in Safety Region Haaglanden hosted all the solution front ends for the individual practitioners. The back-ends (servers) for all participating solutions as well as for the Test-bed were hosted by remote sites and accessed via internet connections:

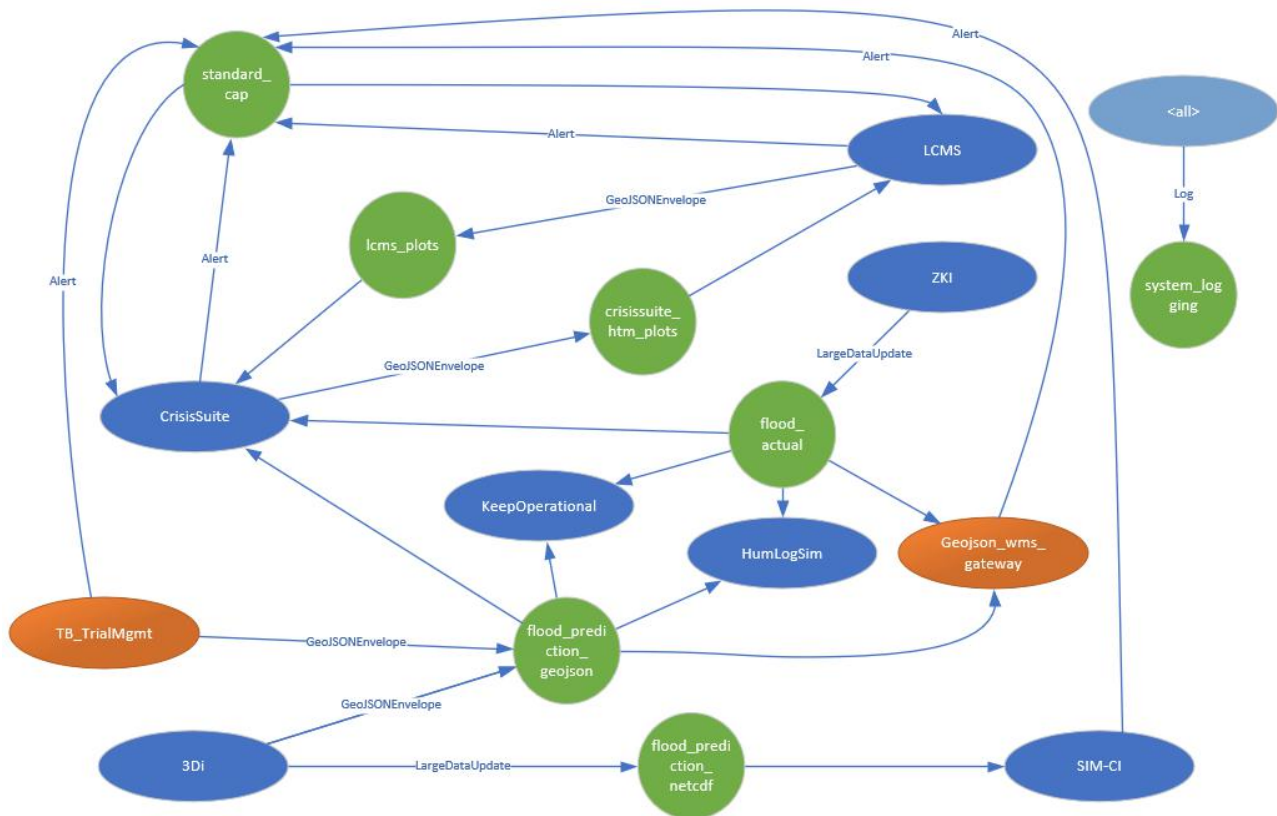
- HUMLOG was hosted by Münster University.
- ZKI and KeepOperational servers were hosted by DLR.
- CrisisSuite was hosted by Merlin.
- SIM-CI was hosted in the cloud.
- 3Di was hosted in the cloud.
- The Test-bed and associated Converters were hosted by TNO in a virtual environment.
- The legacy LCMS is a cloud-based application connected via internet.



**Figure A3.2: Physical deployment of solution back-ends for Trial 4**

### Communication channels configured in the Test-bed

Figure A3.3 provides an overview of the technical integration of the solutions with the Test-bed. The green circles in this figure represent so-called “topics”, which are pre-configured in the Test-bed for this Trial-4 to realise the communication channels between solutions. On one hand, each solution may publish messages of a certain type onto certain topics; on the other hand, each solution may subscribe at certain topics in order to receive all messages that are published on that topic. Just as an example: the 3Di solution publishes “LargeDataUpdate” messages to the “flood\_prediction\_netcdf” topic and “GeoJSONEnvelope” message to the “flood\_prediction\_geojson” topic. Solutions CrisisSuite, KeepOperational and HumLogSim all subscribe to the “flood\_prediction\_geojson” topic – so they will receive all “GeoJSONEnvelope” messages from 3Di solution.



**Figure A3.3: Technical solution integration, using various topics configured in the Test-bed**

As active Test-bed features the following topics have been used in Trial 4:

- Core topics
  - System\_heartbeat (all solutions sending out their “alive” status).
  - System\_admin\_heartbeat (the Admin Tool sending out its “alive” status).
  - System\_logging (logs for all solutions and Admin Tool).
  - System\_topic\_access\_invite (allowing solutions to listen to all standard topics).
  - System\_session\_mgmt (sent by TMT for Session Start/Stop).
  - System\_phase\_message (sent by TMT for new Phase information).
  - System\_role\_player\_message (sent by TMT indicating a Player needs to perform a manual action).
- Standard topics (<https://github.com/DRIVER-EU/avro-schemas/tree/master/standard>):
  - standard\_cap  
CAP: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard\\_cap-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard_cap-value.avsc).
  - flood\_prediction\_netcdf  
Large Data Update: [https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system\\_large\\_data\\_update-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system_large_data_update-value.avsc).
  - flood\_prediction\_geojson  
GeoJSON: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard\\_geojson-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard_geojson-value.avsc) (if too large use the Large Data Update).
  - flood\_actual\_geojson  
GeoJSON: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard\\_geojson-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard_geojson-value.avsc).
  - lcms\_plots  
GeoJSON: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard\\_geojson-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/geojson/standard_geojson-value.avsc).



## Solution Integration Sequence Diagrams

These figures below provide some example sequence diagrams created automatically out of the recordings produced by the After-Action Review tool during the execution of Trial 4 on 22-23/05/2019. More information is available online on <http://134.221.20.201:8199/#/>.

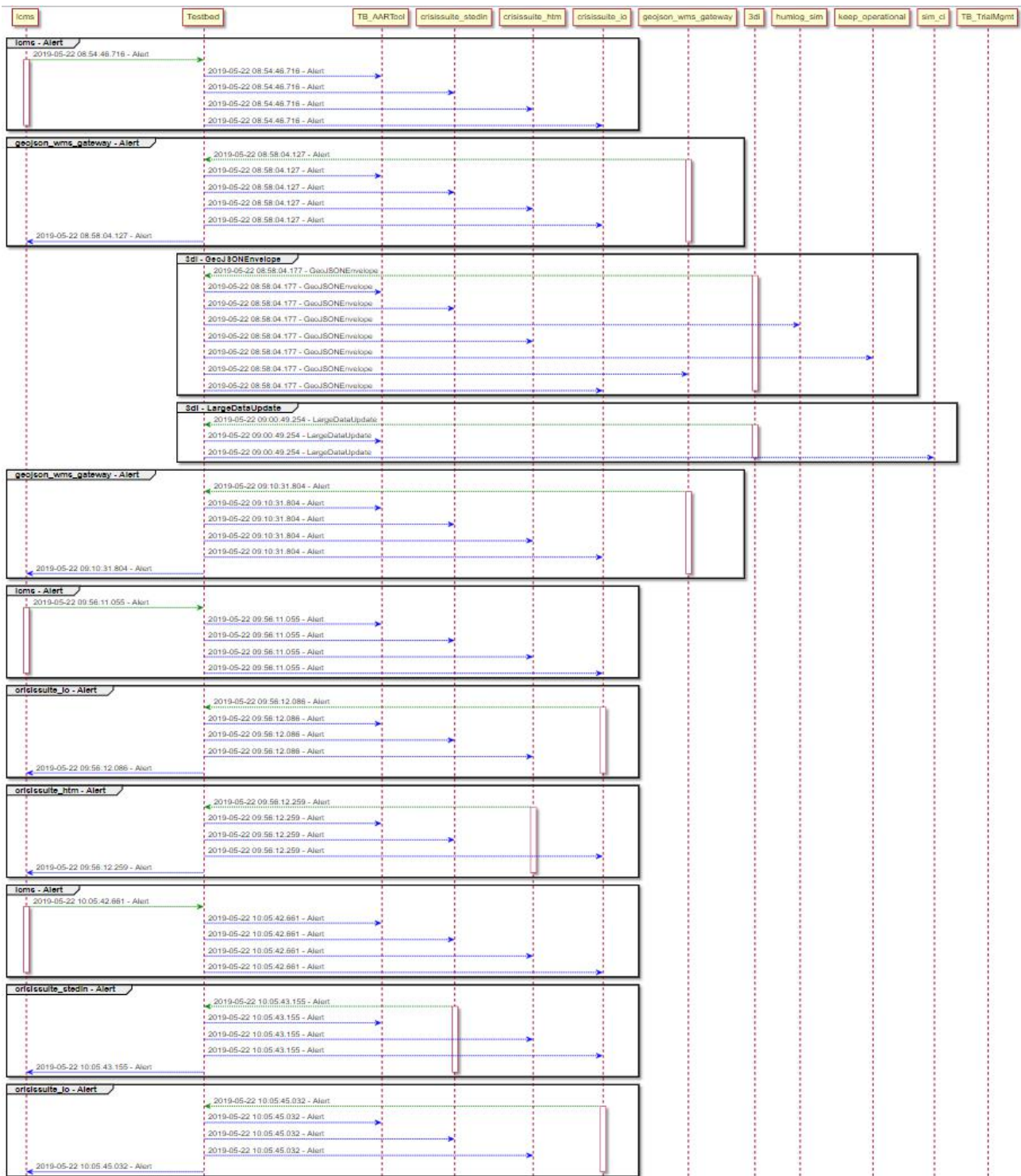


Figure A3.4: Trial 4 - Block 1 sequence diagram – example extract

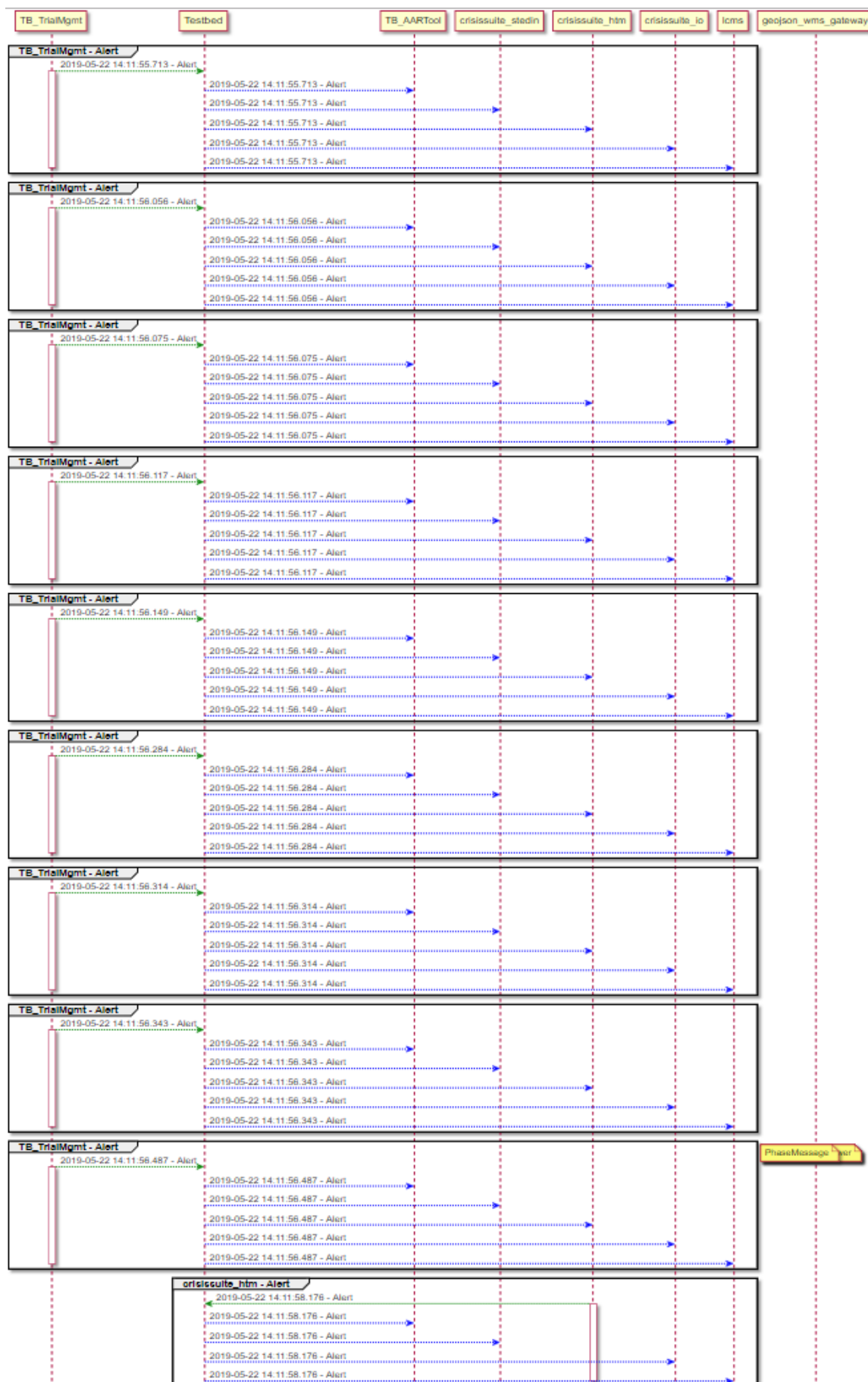


Figure A3.5: Trial 4 - Block 2 sequence diagram – example extract



## Solution Integration – Test-bed messages

This section provides examples of messages as they were recorded by the After-Action Review tool during the execution of Trial 4 on 22-23/05/2019. All recordings are available online on <http://134.221.20.201:8199/#/>.

**Table A3.1: Trial 4 – LargeDataUpdate message example**

LargeDataUpdate Message	
Sender	3Di
Topic	flood_prediction_ncdf
Message content	<p>Record ID: 1977</p> <p>Headline: null</p> <p>URL: <a href="https://demo.lizard.net/api/v3/scenario-results/65995/results_3di.nc">https://demo.lizard.net/api/v3/scenario-results/65995/results_3di.nc</a></p> <p>Data Type: netcdf</p> <p>Title: b1_trial4_1230u_100m3s_raw_3Di_output</p> <p>Description: raw_3Di_output</p> <p>Attachments:</p>

**Table A3.2: Trial 4 – Log message example**

Log Message	
Sender	KeepOperational
Topic	system-logging
Message content	<p>Record ID: 2307</p> <p>Headline: --&gt; addCallback: flood_prediction_geojson</p> <p>Client ID: keep-operational</p> <p>Date/Time: 2019-05-23 09:42:02.362</p> <p>Level: INFO</p> <p>Message: --&gt; addCallback: flood_prediction_geojson</p> <p>Attachments:</p>

**Table A3.3: Trial 4 – GeoJSON message example**


GeoJSON Message	
Sender	3Di
Topic	flood_prediction_geojson
Message content	<p>Record ID: 1543</p> <p>Map:</p>  <p>Headline: null</p> <p>Client ID: 3di</p> <p>Date/Time: 2019-05-22 08:58:04.177</p> <p>Level:</p> <p>Attachments:</p> <p>Message:</p> <pre> ▼ : Object[2]   ▼ properties: Object[3]     name: "b1_1100_predicted_3di"     src_url:       "https://demo.lizard.net/media       /downloads/e642c836-f5a5-43c2-815a-       60824bb1b523/b1_trial14_1230u_100m3s-       water-depth-       timeseries_20160105T151451Z.tif"     dataType: "geojson"   ▼ geojson: Object[3]     type: "FeatureCollection"     bbox: null     features: Array[567]       ▼ 0: Object[4]         type: "Feature"         bbox: null         geometry: Object[2]           type: "Polygon"           coordinates: Array[1]             ▼ 0: Array[5]               ▼ 0: Array[2]                 0: 4.3021                 1: 52.0996               ▼ 1: Array[2]                 0: 4.3021                 1: 52.0994               ▼ 2: Array[2]                 0: 4.3017           </pre> <p>... and many more lines ...</p>

Table A3.4: Trial 4 – Alert message example

Alert Message	
Sender	CrisisSuite
Topic	standard_cap
Message content	<div> Record ID: 3058   Headline: Informatie versturen naar LCMS   Sender: stedin@crisis suite.com   Date/Time: 2019-05-23 15:01:29.732   Attachments:   Message:  ▼ : Object[14]      identifier:        "bac70d42-9a19-45d9-a9d8-bdb529f2d958"      sender: "stedin@crisis suite.com"      sent: "2019-05-23T15:01:29+02:00"      status: "Exercise"      msgType: "Update"      source: null      scope: "Public"      restriction: null      addresses: null      code: "crisis suite_sitrep"      note: null </div> ... and many more lines ...

## Annex 4 – Final Demonstration – Technical details

This annex provides some technical details related to the Final Demonstration.

### Data Exchange Diagram

Figure A4.1 provides an overview of which kind of data was exchanged between which solutions, using which Standards, in the scope of which test cases, during the Final Demo.

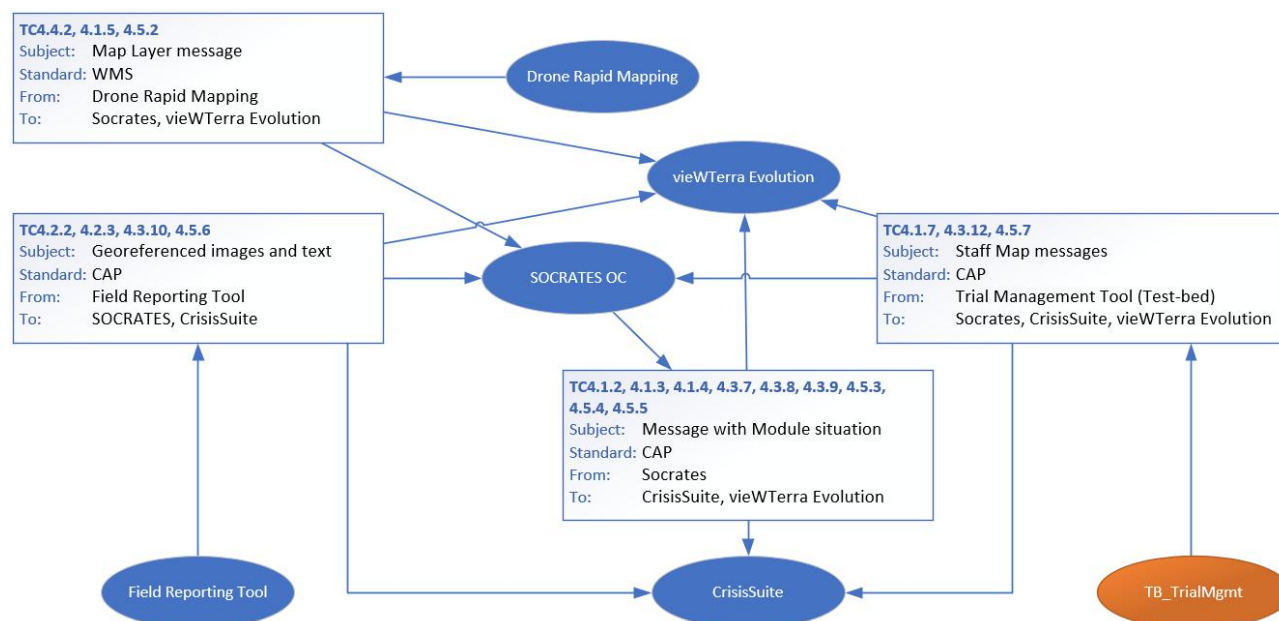
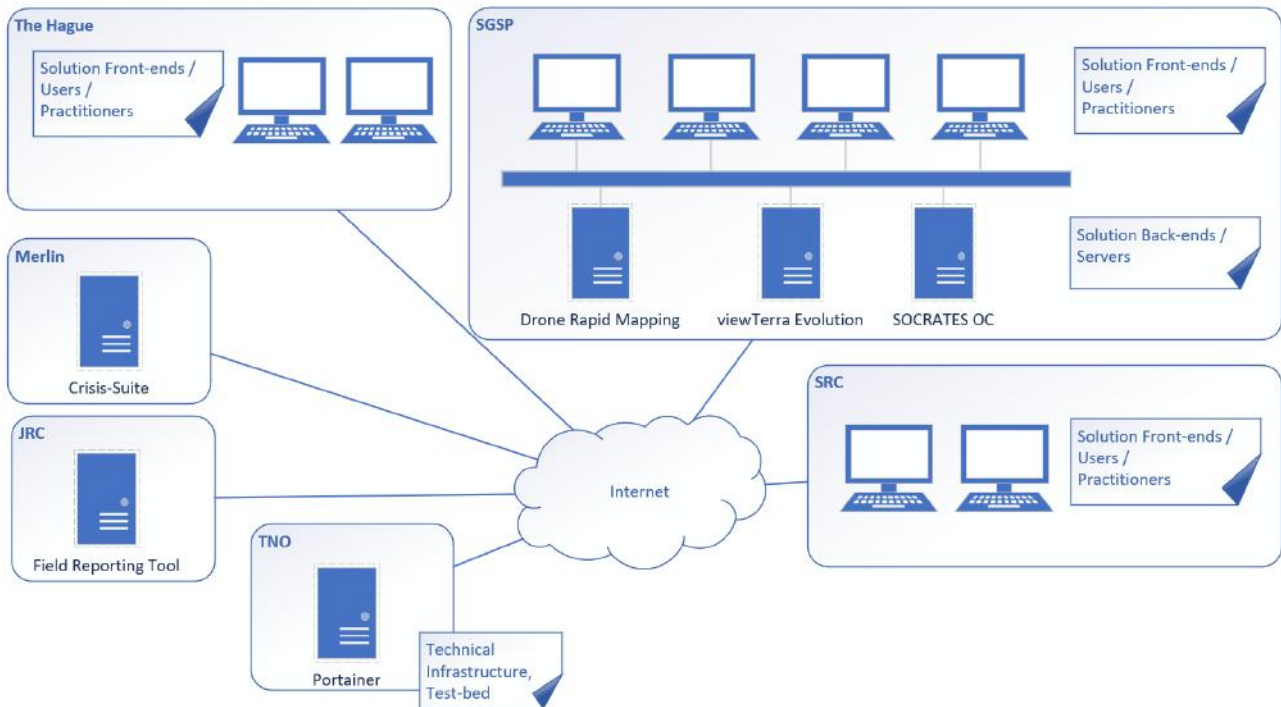


Figure A4.1: Data Exchange Diagram of the Final Demo

### Solution and Test-bed deployment

The physical deployment of computer infrastructure (clients and servers) used by the solutions for the Final Demo is visualized in Figure A4.2. This figure illustrates that the technical integration of solutions for the Final Demo was highly distributed. Solution front-ends (clients) were available at all three locations, two in Warsaw (at SGSP and SRC) and one in The Hague (SRH). The back-ends (servers) for solutions Drone Rapid Mapping, viewTerra Evolution and SOCRATES OC were located at SGSP, while the servers of other solutions as well as the Test-bed were remotely accessed via internet connections to Merlin (CrisisSuite solution), JRC (Field Reporting Tool solution) and TNO (Test-bed).

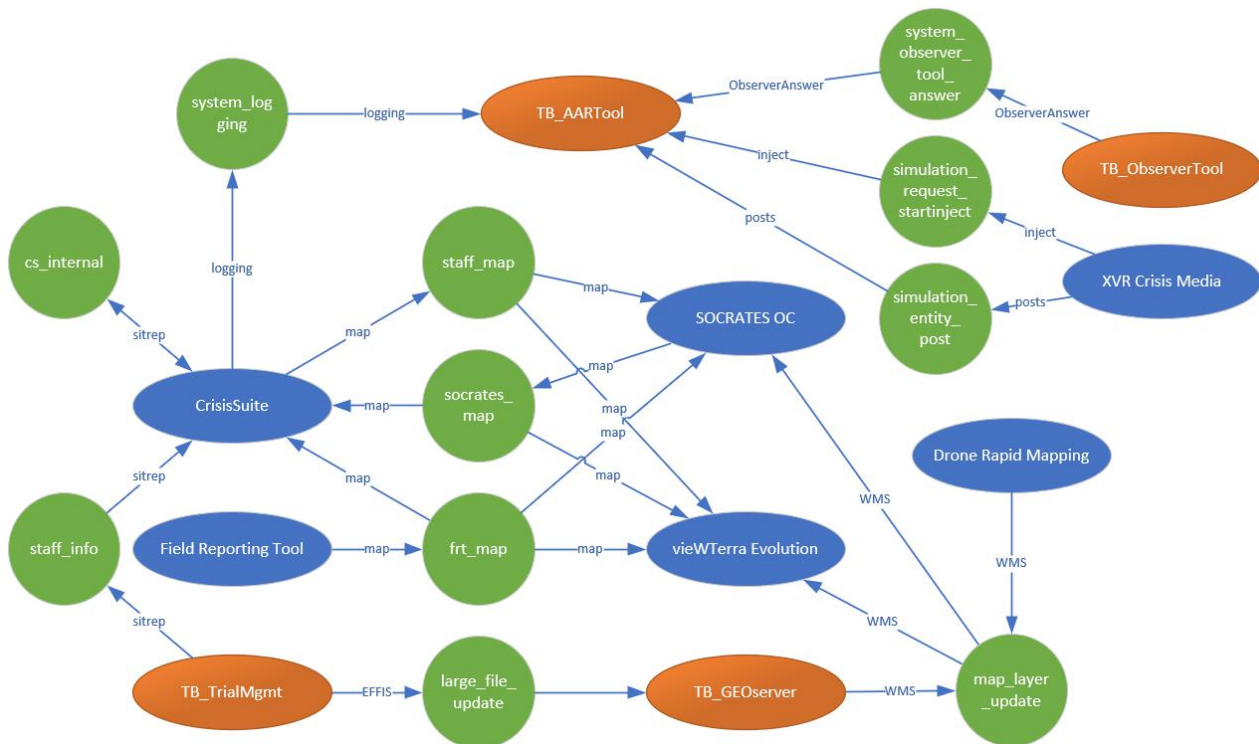


**Figure A4.2: Physical deployment of solution back-ends for the Final Demo**

#### Communication channels configured in the Test-bed

Figure A4.3 provides an overview of the technical integration of the solutions with the Test-bed. The green circles in this figure represent so-called “topics”, which are pre-configured in the Test-bed for this Final Demo Trial to realise the communication channels between solutions. On one hand, each solution may publish messages of a certain type onto certain topics; on the other hand, each solution may subscribe at certain topics in order to receive all messages that are published on that topic. Just as an example: the SOCRATES OC solution publishes “map” messages to the “socrates\_map” topic. Solutions CrisisSuite and viewTerra subscribe to the “socrates\_map” topic – so they will receive all “map” messages from SOCRATES OC solution.

Note that not also some Test-bed infrastructure components (not only solutions) make use of the topic for data exchange: examples are TB\_TrialMgmt, TB\_GEOserver.



**Figure A4.3: Technical solution integration, using various topics configured in the Test-bed**

As active Test-bed features the following topics have been used in the Final Demo:

- Core topics
  - System\_heartbeat (all solutions sending out their “alive” status).
  - System\_admin\_heartbeat (the Admin Tool sending out its “alive” status).
  - System\_logging (logs for all solutions and Admin Tool).
  - System\_topic\_access\_invite (allowing solutions to listen to all standard topics).
  - System\_session\_mgmt (sent by TMT for session start/stop).
  - System\_phase\_message (sent by TMT for new phase information).
  - System\_role\_player\_message (sent by TMT indicating a player needs to perform a manual action).
  - System\_ost\_answer (sent by OST – Observer Answers)
- Standard topics (<https://github.com/DRIVER-EU/avro-schemas/tree/master/standard>):
  - large\_data\_update  
Large Data Update: [https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system\\_large\\_data\\_update-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system_large_data_update-value.avsc).
  - map\_layer\_update  
Map Layer Update: [https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system\\_map\\_layer\\_update-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/core/large-data/system_map_layer_update-value.avsc).
  - cs\_internal  
CAP: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard\\_cap-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard_cap-value.avsc).
  - staff\_map  
CAP: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard\\_cap-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard_cap-value.avsc).
  - socrates\_map  
CAP: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard\\_cap-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard_cap-value.avsc).
  - frt\_map  
CAP: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard\\_cap-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard_cap-value.avsc).

- staff\_info
- CAP: [https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard\\_cap-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/standard/cap/standard_cap-value.avsc).
- simulation\_entity\_port
- Post: [https://github.com/DRIVER-EU/avro-schemas/blob/master/sim/entity/simulation\\_entity\\_post-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/sim/entity/simulation_entity_post-value.avsc)
- simulation\_request\_startinject
- RequestStartInject: [https://github.com/DRIVER-EU/avro-schemas/blob/master/sim/request/simulation\\_request\\_startinject-value.avsc](https://github.com/DRIVER-EU/avro-schemas/blob/master/sim/request/simulation_request_startinject-value.avsc).

## Solution Integration Sequence Diagrams

This annex provides example sequence diagrams created automatically out of the recordings produced by the After-Action Review tool during Dry Run 2 of the Final Demonstration on 26/09/2019. More information is available online on <http://134.221.20.201:8299/#/>.

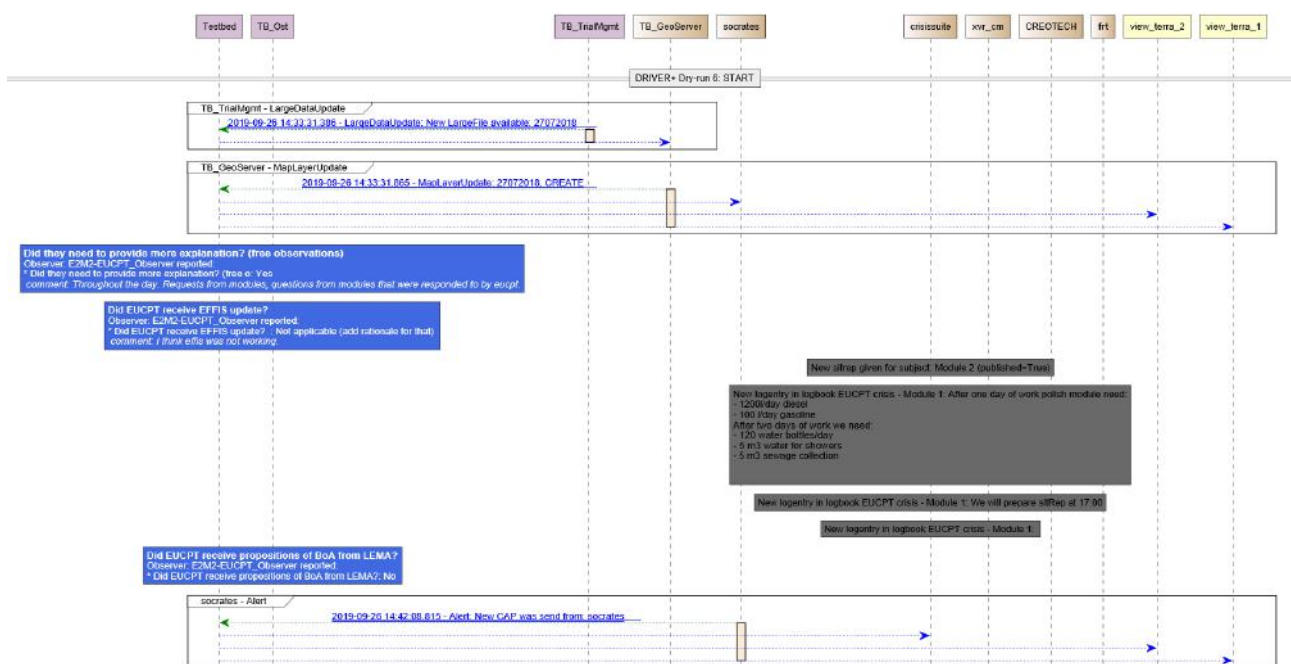


Figure A4.4: Final Demo, Dry Run 2 example sequence diagram (extract)

## Solution Integration – Test-bed messages


This section provides examples of messages as they were recorded by the After-Action Review tool during Dry Run 2 of the Final Demonstration on 26/09/2019. All recordings are available online on <http://134.221.20.201:8299/#/>.



**Table A4.1: Final Demo – LargeDataUpdate message example**

LargeDataUpdate Message	
Sender	TB_TrialManagement
Topic	large_data_update
Message content	<p>Record ID: 614</p> <p>Headline: New LargeFile available: 17072018_1011</p> <p>URL: <a href="http://tb3.driver-testbed.eu/files/17072018_1011.tif">http://tb3.driver-testbed.eu/files/17072018_1011.tif</a></p> <p>Data Type: image_geotiff</p> <p>Title: 17072018_1011</p> <p>Description: 63.137021,14.081303242,61.215546167</p> <p>Attachments: <a href="#">record/attachements/17072018_1011.tif</a></p>

**Table A4.2: Trial 4 – Alert message example**

Alert Message	
Sender	CrisisSuite
Topic	frt_map
Message content	<p>Record ID: 933</p> <p>Map:</p>  <p>Headline: no-reply@crisissuite.com + FRT,8431ff59-a04c-4dd9-a582-3ef0f3609fe1,2019-09-26T16:03:00Z</p> <p>Sender: no-reply@crisissuite.com</p> <p>Date/Time: 2019-09-26 16:04:01.663</p> <p>Attachments:</p> <p>Message:</p> <pre>: Object[14]   identifier:     "16fe0d15-6a8f-4c1c-a8f2-4a7e999d7e58"   sender: "no-reply@crisissuite.com"   sent: "2019-09-26T16:04:02+02:00"   status: "Exercise"</pre>

## Annex 5 – Integration reports of non-selected internal solutions

---

### A5.1 Rumour Debunker

---

Use Cases and Test Cases for the Rumour Debunker solution are presented in section 6.3.1. This annex presents the corresponding test report.

#### Execute Tests and Reports

How was the connection to the Test-bed tested and what were the results?

The tests consisted of sending several News requests. The backend adapter has been loaded and a report for a Rumour Debunker script has been created, after the user sent a request. The report has then been sent to the Test-bed and the Kafka-adapter has been monitored if the message has been successfully sent.

Then the console log has been checked whether or not the Kafka-adapter has accepted the message. In the next step, the “External Data Hub” has been checked if the message (HelloWorld) has been displayed. If it has been displayed, the test was successful, the console log has been stored and the process can begin anew.

To complete the process, a full stream of operational data is sent from Rumour Debunker repository to the Test-bed. The log is documented in screen shoots.

The Rumour Debunker client is an android application which is developed to show the newest quality checked news.

#### Test Results

Rumour Debunker is a solution from DRIVER+ partner AIT. This solution uses the NodeJS adapter to connect to the Test-bed.

Rumour Debunker has been integrated into the Test-bed with the provided solutions on the project’s Github page. It utilises the NodeJS adapter. This was successfully installed by first

- Installing the Docker environment (which also allowed for local testing) and then, in a next step.
- Installing all the appropriate software components.

Initially, a local distribution of the Test-bed was installed to see what adjustments to the solution structure and code were required to enable a “HelloWorld”-test integration. These adaptations consisted of first implementing the handling of incoming messages on the NodeJS Script. For this purpose, a new class “Test-bed integration” was created. Further, a logging system has been set up that now writes warning, errors and further program information with the appropriate time stamp in a .txt-file.

After ensuring the system can receive messages according to the DRIVER+ Test-bed format, the next step was to adapt the solution to forward messages to the interface and display them on the project page. This required the migration from the previously used JSON to the required AVRO schema, as well as some small front-end adaptations to allow the “HelloWorld”-message to be displayed.

After this adaptation, the testing process has begun to ensure uninterrupted communication. For this purpose, the individual process was started first and then a message was sent via the adapter. After the adapter received the event, the message was displayed. The logging-system was then consulted to see if any errors occurred during the process.

Currently, the system can exchange messages with itself according to the required DRIVER+ standard. Further tests are performed to ensure both stability and consistency.

The following back-end adaptations have been performed on the solution for the Test-bed integration:

- Installation of the NodeJS adapter to connect to the Test-bed (<https://github.com/DRIVER-EU/node-Test-bed-adapter>).
- Installation of the required Docker container and required services (<https://github.com/DRIVER-EU/Test-bed>).
- Installation of DRIVER+ TypeScript adapter on the CrowdTasker backend.
- Installation and testing of the Kafka Test-bed to forward messages to the interface.
- Installation of local Test-bed solution (for initial testing purposes).
- Adaptation of the existing solution to forward messages to the interface.
- Adaption of existing NodeJS Script to handle incoming messages (internal processing).
- Migration from JSON scripts to the required AVRO schema.
- Creation of logging system.

The following front-end adaptations have been performed on the solution for the Test-bed integration:

- Adaption of the existing homepage to display “Hello World” message.

The following IT infrastructure related work has been performed during the Test-bed integration process:

- Opening required ports to grant DRIVER+ access to server.
- Installation of required packages.
- Testing access from different crucial connection points.

The testing process of the Test-bed integration consists of the following steps:

- Start of Docker container.
- Start of adapter.
- Adapter sends test message/event (rumour\_debunker\_hello\_world-value.avsc).
- Check log if report has been sent.
- Adapter receives test event.
- Check log if report has been received without any errors.
- Adapter verifies content of message.
- Adapter displays “Hello World”.
- Check if “Hello World” message is displayed on homepage.

Next step sending quality checked messages from Rumour Debunker to the Test-bed. (Rumour Debunker is acting as producer and the Test-bed is the consumer).

An example screen shot from the sending client (Android app) is visualised in Figure A5.5.

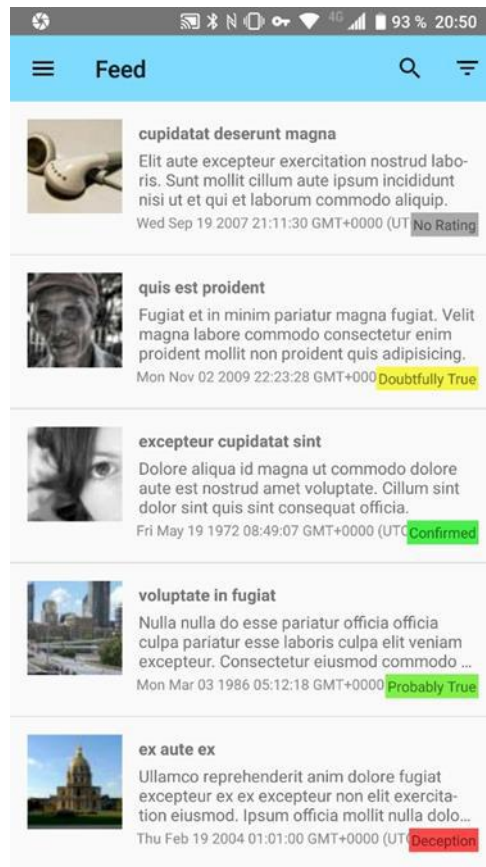


Figure A5.5: Example Screenshot (Android App)

The intention for Rumour Debunker development after DRIVER finalization is to continue testing and improving the solution and to finally provide the result for operational use.

## A5.2 Protect

The integration of Protect solution is described in section 6.3.2. This annex presents the test report of the Protect solution integration in form of screen shots.

Usage of the Docker Engine is visualised in Figure A5.6 to Figure A5.8.

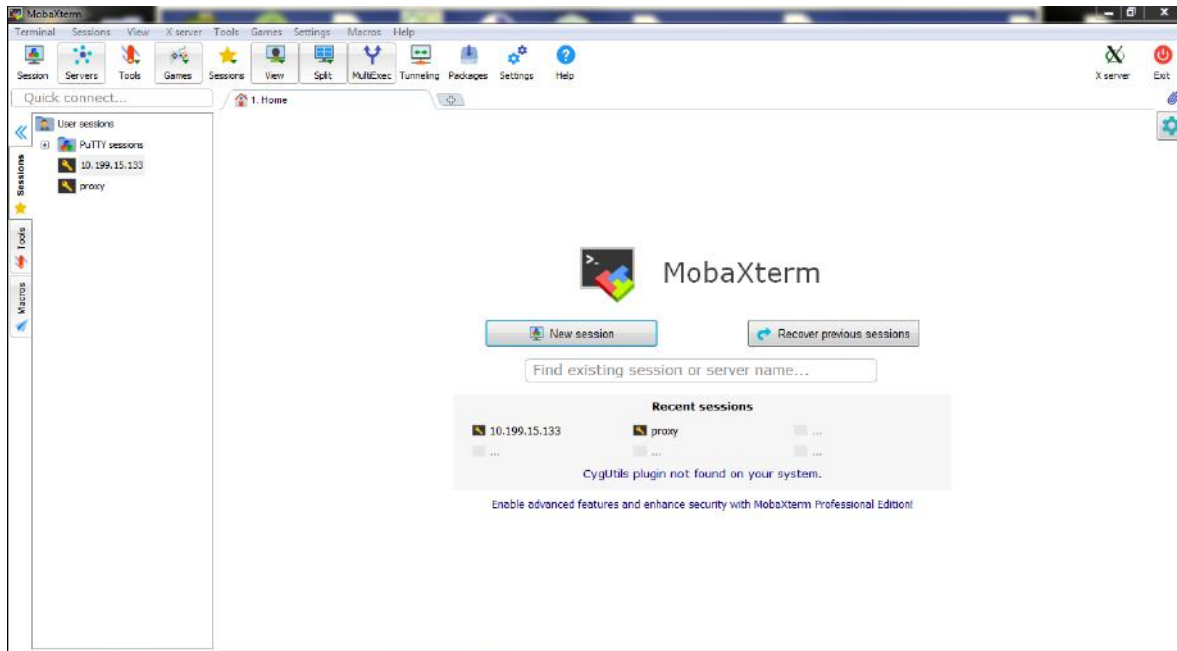


Figure A5.6: Docker Engine

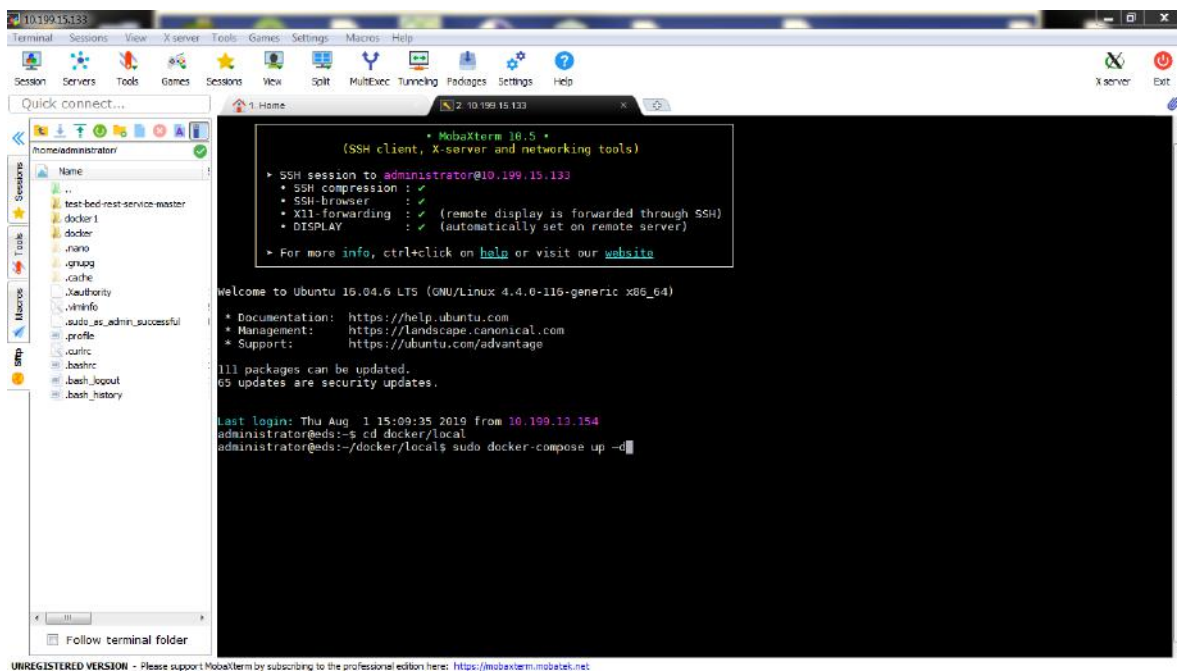


Figure A5.7: Docker Engine (2)

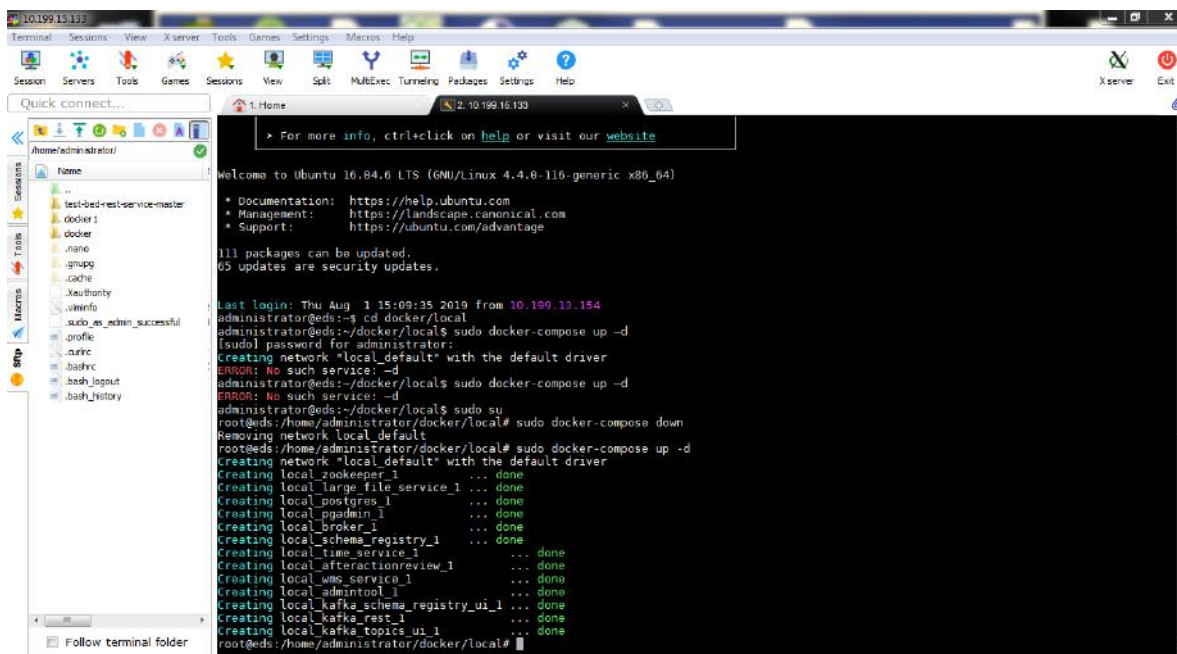


Figure A5.8: Docker Engine (3)

## Test bed version 1.2.8 jar

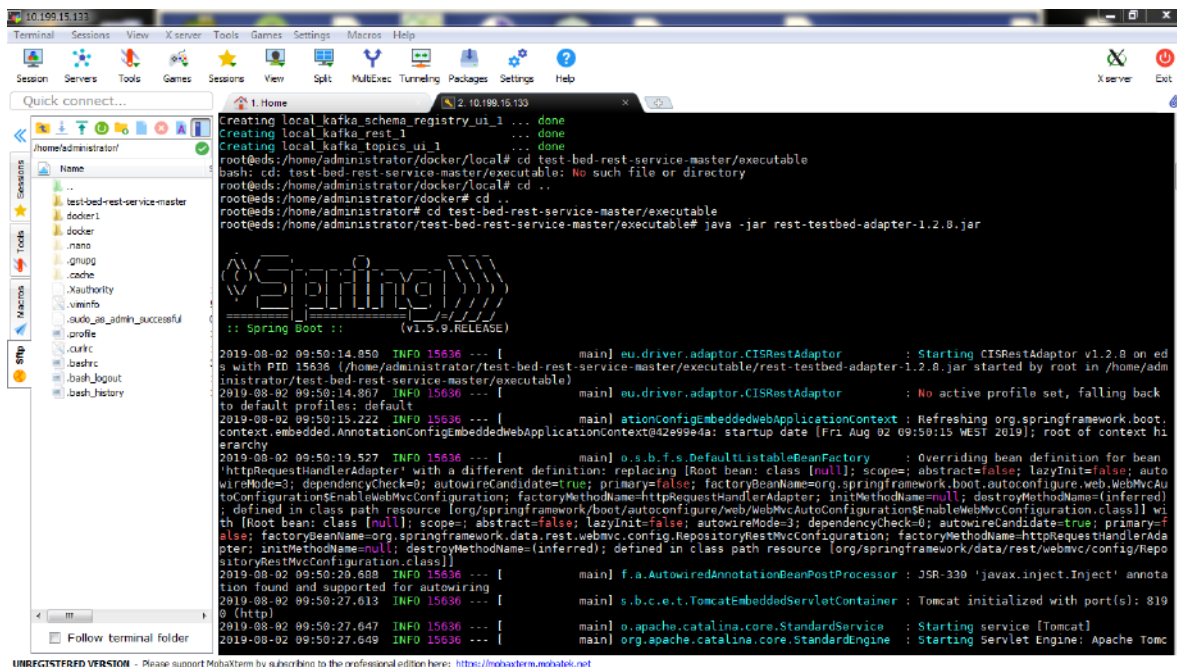


Figure A5.9: Test bed version 1.2.8 jar



Protect:

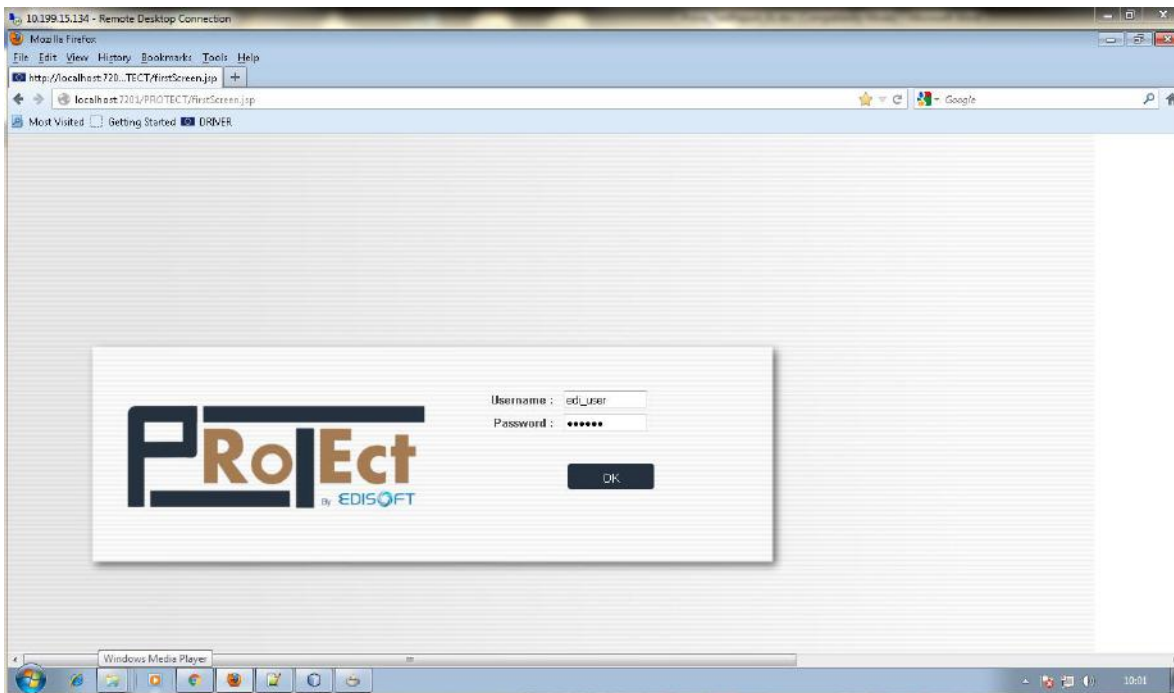


Figure A5.10: Protect

Add Rest End Point:

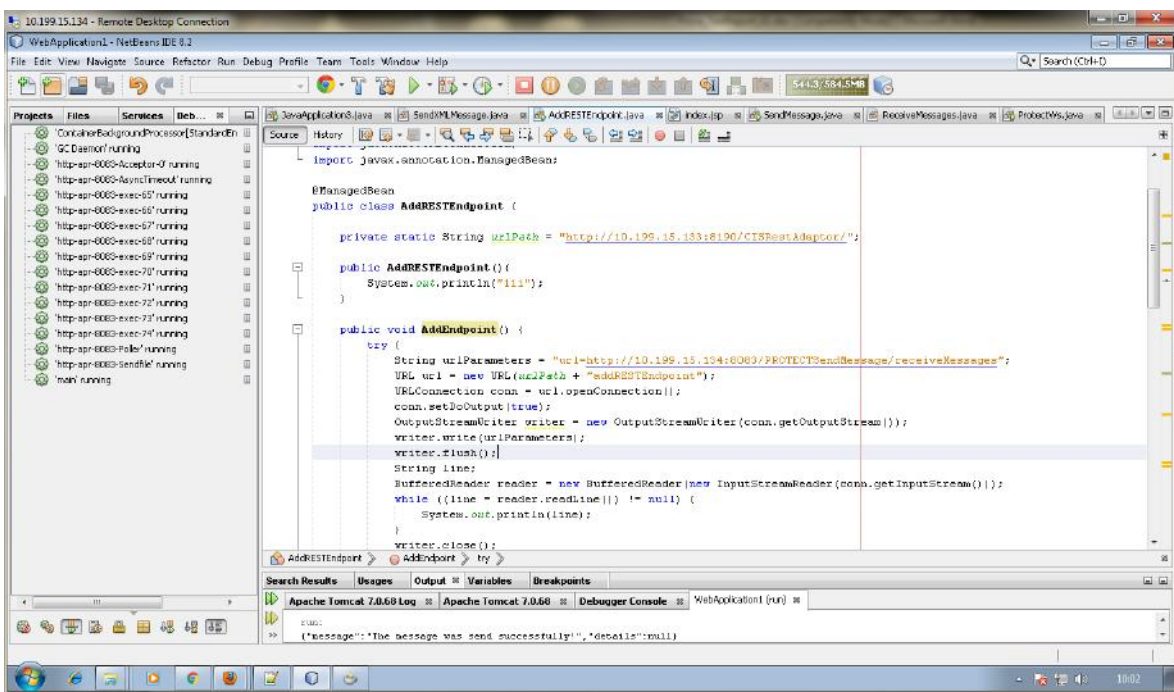


Figure A5.11: Protect Rest adapter End Point developed from the start



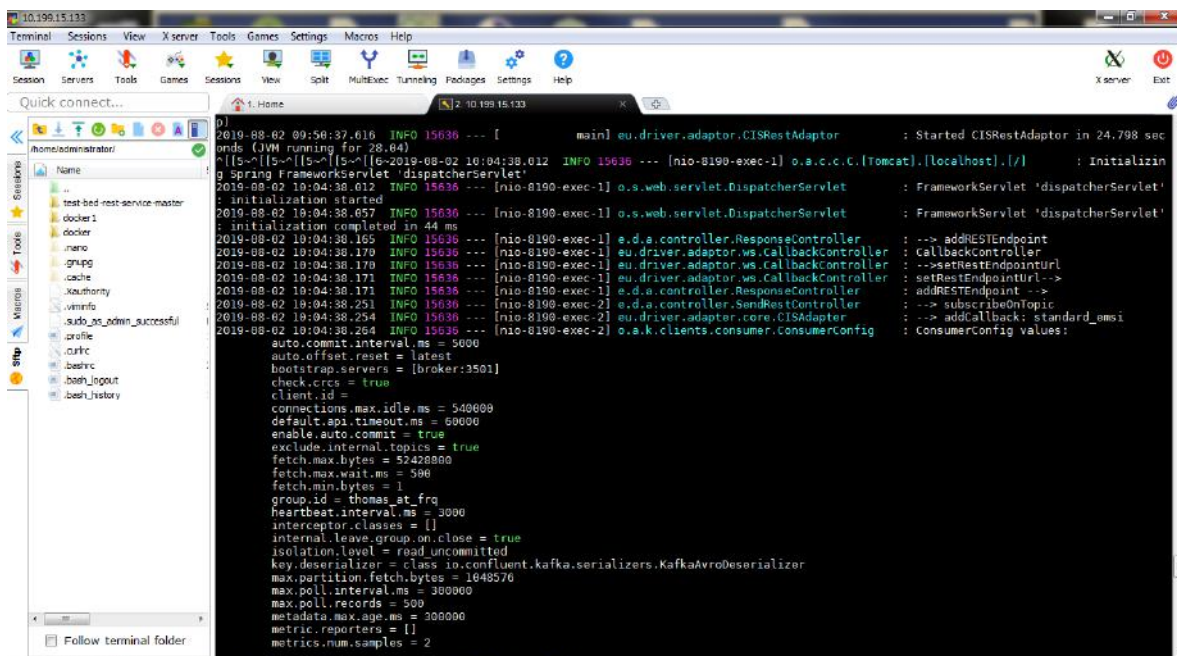


Figure A5.12: Result of the received message in the Test Bed

Result of the sent message in Protect Endpoint:

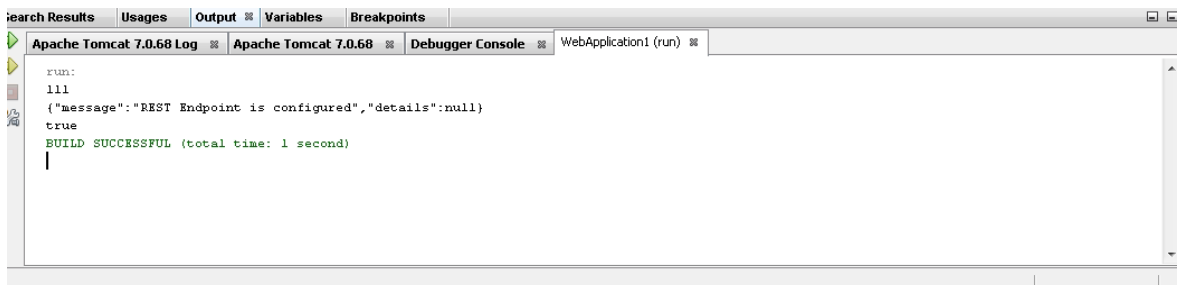


Figure A5.13: Result of the sent message in Protect Endpoint

EMSI message from Protect

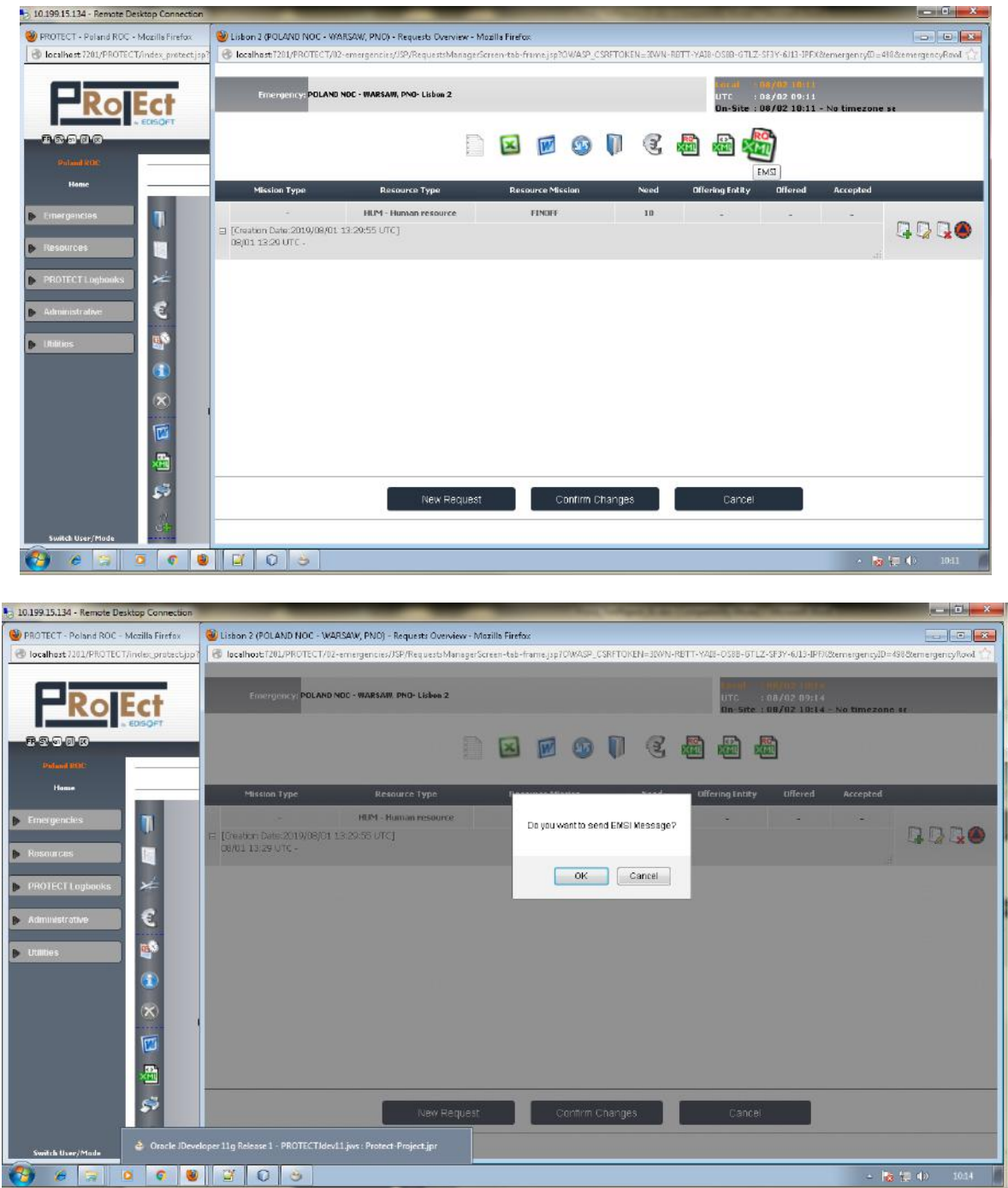
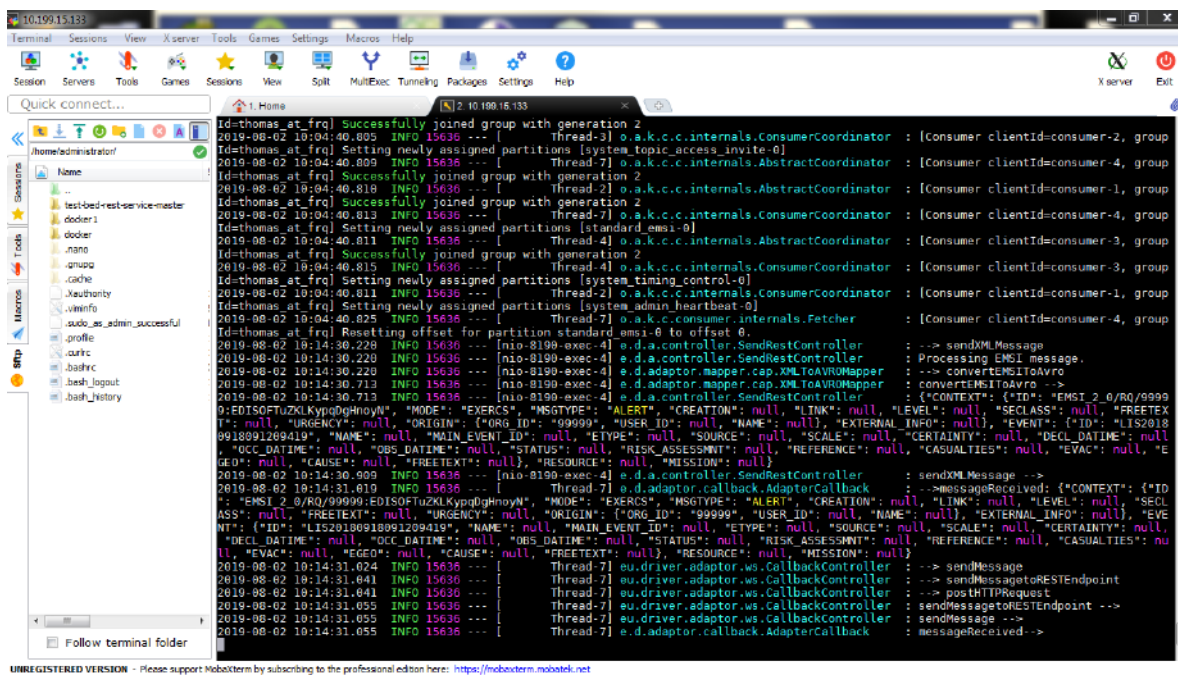
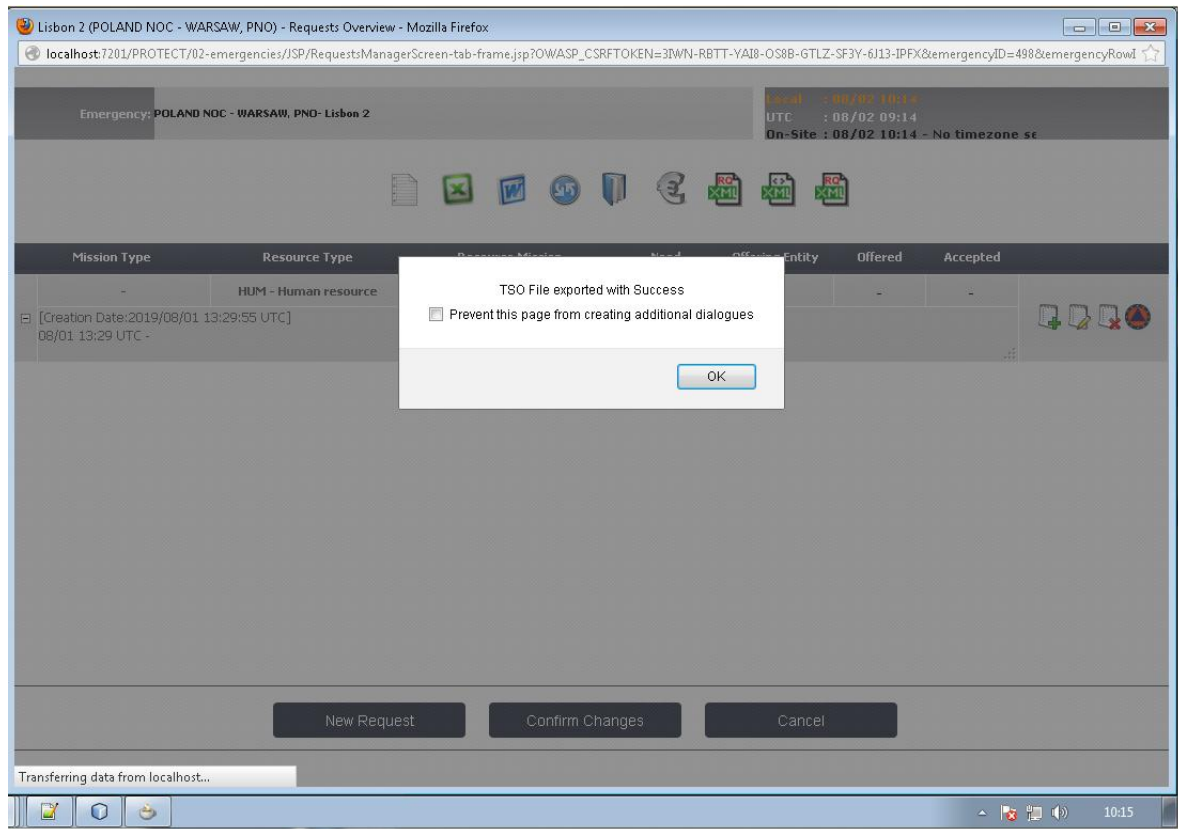


Figure A5.14: Protect sending a EMSI message



**Figure A5.15: Message sent from Protect and received in Test Bed**

## Receiving a message in Protect from another entity using the Test Bed

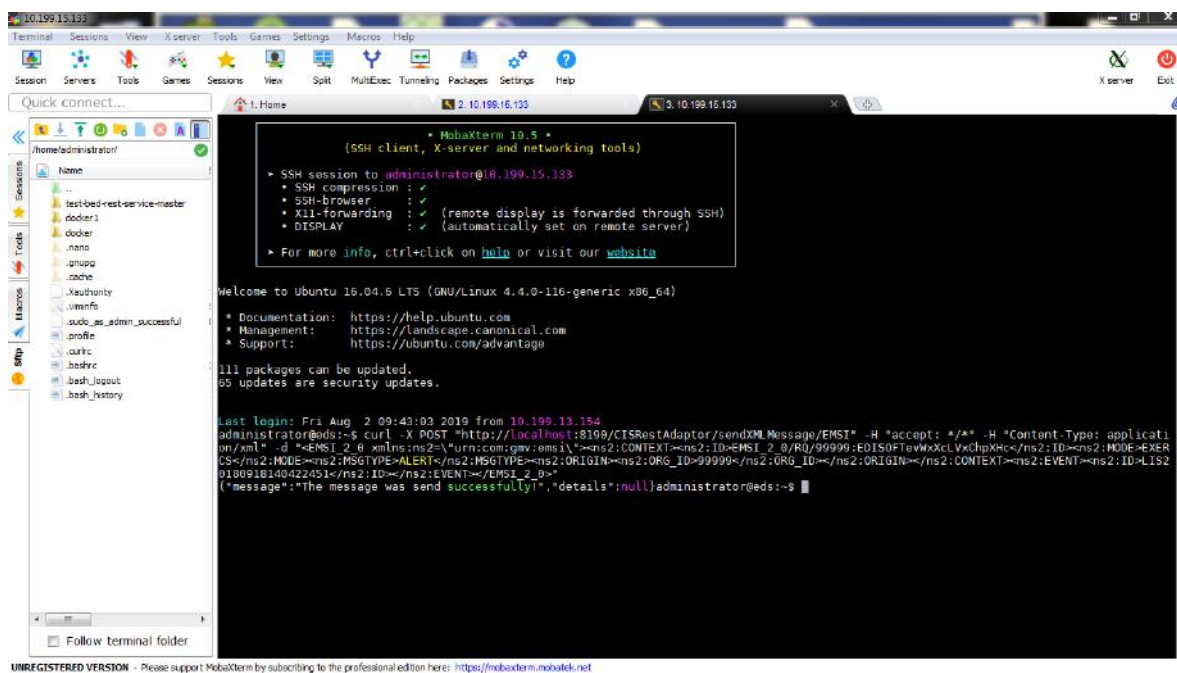


Figure A5.16: Doing a curl command with a EMSI message in the Test Bed

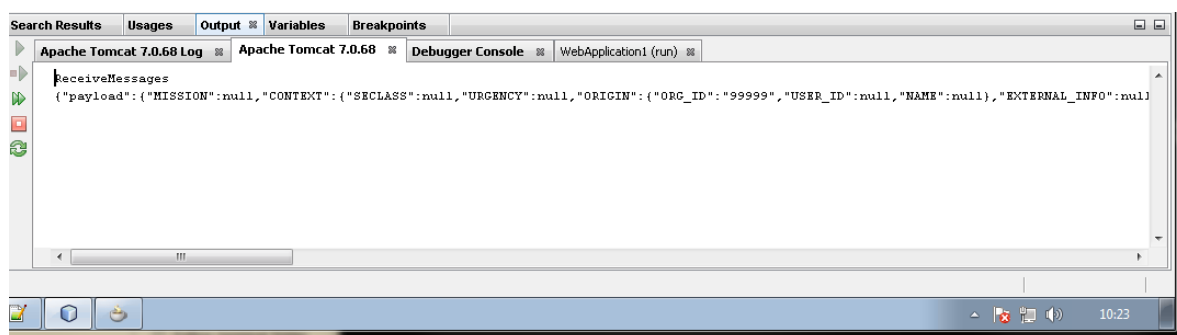


Figure A5.17: Received message in Protect End point

## A5.3 IO-DA

---

The Use Cases for the IO-DA solution are presented in section 6.3.3. This annex presents the corresponding test scenario and test report.

### Test scenario corresponding to the use cases

#### **TS #1a – Sharing of data**

Related use case: UC #1 – Get a complete situation overview of the crisis, with the context, stakeholders, and objectives.

IO-DA has a knowledge database comporting all the information about the geographical context of a given area, and the stakeholders able to intervene in any crisis occurring in this given area. This knowledge database will be completed thanks to a file provided by solution B. This file must comport the objectives of the crisis, which means the alerts of the crisis, along with information about them such as the localization, urgency, category, etc. This file will be sent in a CAP format.

IO-DA must provide a mapping in order to change the format of the file from CAP to XML so that IO-DA is able to integrate the data into its knowledge database.

Description and objective:

An alert file is generated by solution B and send to IO-DA via the Test-bed. The information contained in this file must be integrated into the knowledge database of IO-DA.

#### **TS #1b – Visualization of data**

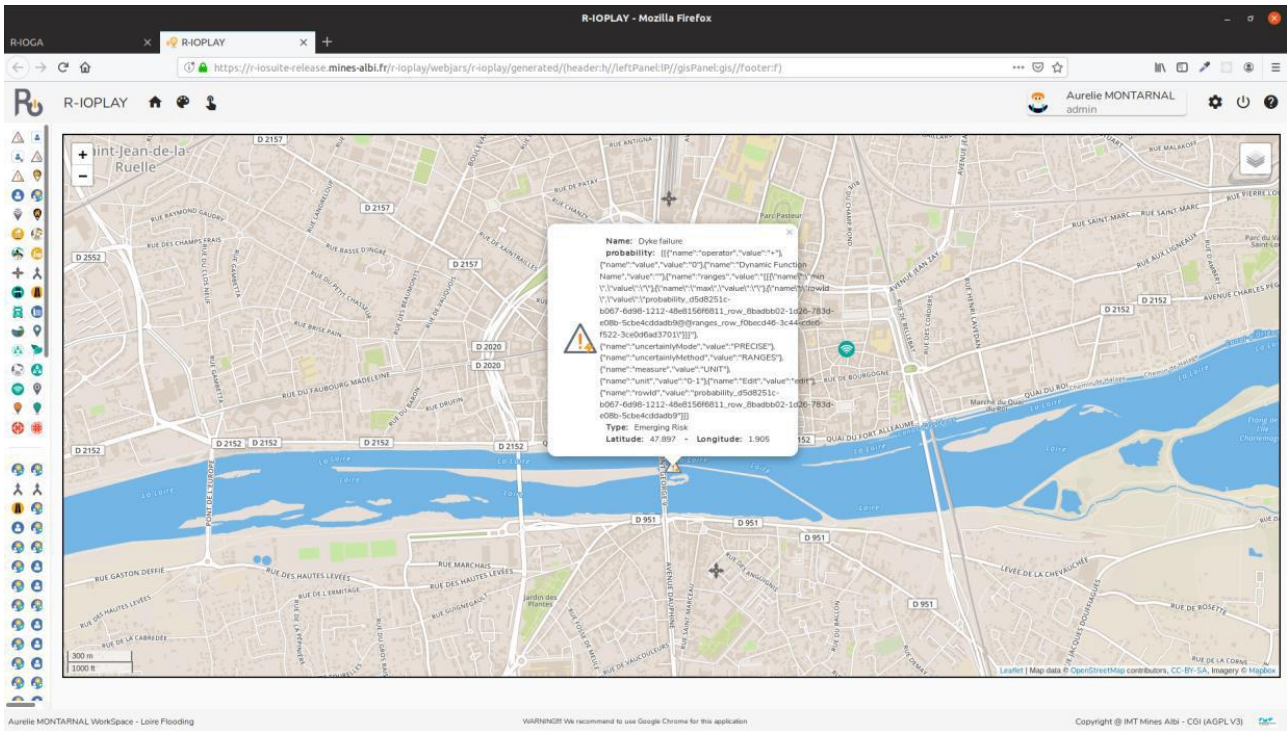
Related use case: UC #1 – Get a complete situation overview of the crisis, with the context, stakeholders, and objectives.

The completed knowledge database of IO-DA can be displayed on a map in order to get an easy and global comprehension of the crisis situation.

Description and objective:

The data shared by LifeX is received and properly displayed on a map by IO-DA.





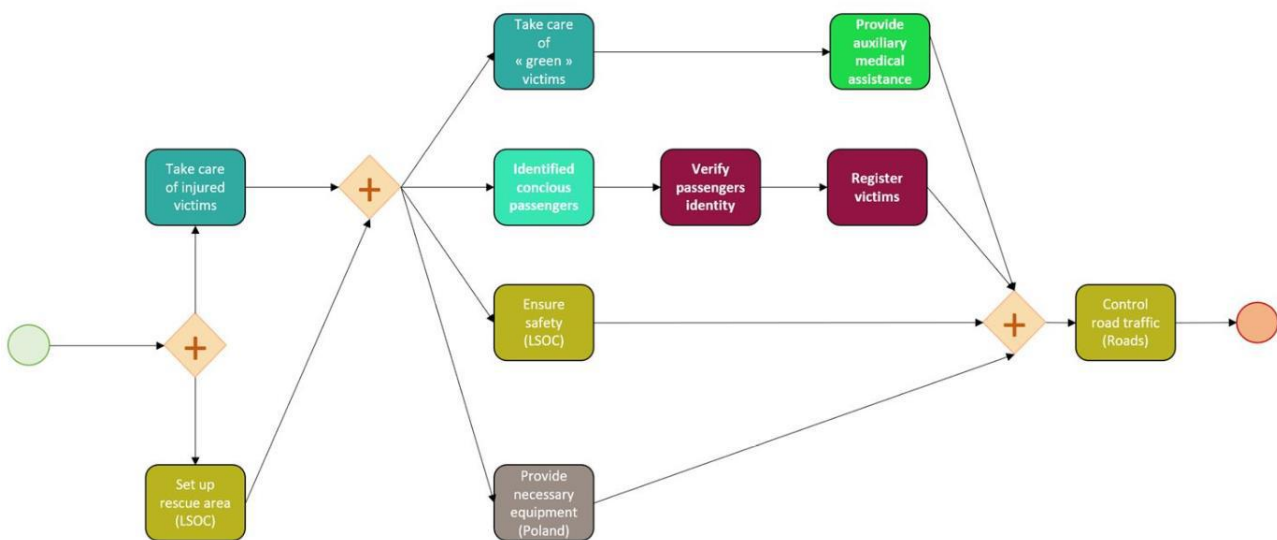
**Figure A5.18: IO-DA's GIS completed with the risks sent into the CAP alert file from another solution**

## TS #2a – Decision help

Related use case: UC #2 – Get decision help.

Thanks to the knowledge database completed by solution B, IO-DA will be able to provide a process about how to best solve the crisis. This process must be in BPMN format. It presents the different actions to be performed by the stakeholders, and in which order, so as to solve the crisis in the most efficient way.

The figure below presents an example of the process provided by IO-DA.



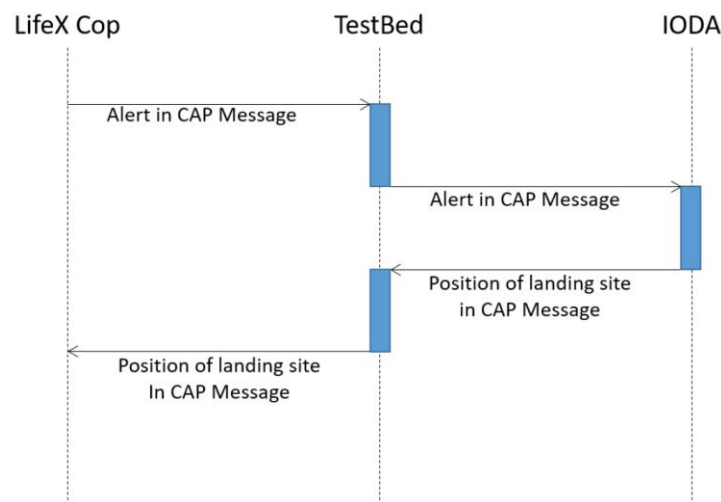
**Figure A5.19: BPMN process deduced by IO-DA from the information available on the crisis in the database**

### Description and objective:

IO-DA generates a BPMN process, changes it into a JSON file and shares it with the Test-bed. The image data shared by LifeX is received and properly displayed in IO-DA. Technical details for displaying in IO-DA: max. delay for displaying, min. resolution, accuracy, symbols to be used etc. (see IO-DA Meta model).

### UML Diagram

The figure below shows a typical sequence diagram. In this case, the solution integrated is LifeX Cop and IO-DA. LifeX Cop sends a message to IO-DA via the Test-bed, and IO-DA sends back another message to the Test-bed.



**Figure A5.20: BPMN process deduced by IO-DA from the information available on the crisis in the database**

### Test Report

A local version of the Test-bed was installed in order to execute the tests and initialised the connection. The idea was to be able to get information from another solution via the Test-bed, to be able to display that information on a map in IO-DA, to use that information in order to generate a process explaining how to solve the crisis, and then to change this process into a JSON file that would be sent to another solution via the Test-bed.

#### TR #1a – Sharing of data

1. IO-DA administrator successfully logs in.
2. IO-DA administrator successfully gets the contextual information about the situation from its own database on a GIS (see Figure A5.21).
3. IO-DA successfully receives an alert file in CAP via the Test-bed, and successfully integrates this alert into its database. The idea is that this alert file would be sent by another solution. An example of the kind of files that LifeX could send to IO-DA is available, and that file is used to make the tests (see Figure A5.22).
4. This information is successfully integrated into IO-DA's database (see Figure A5.23).



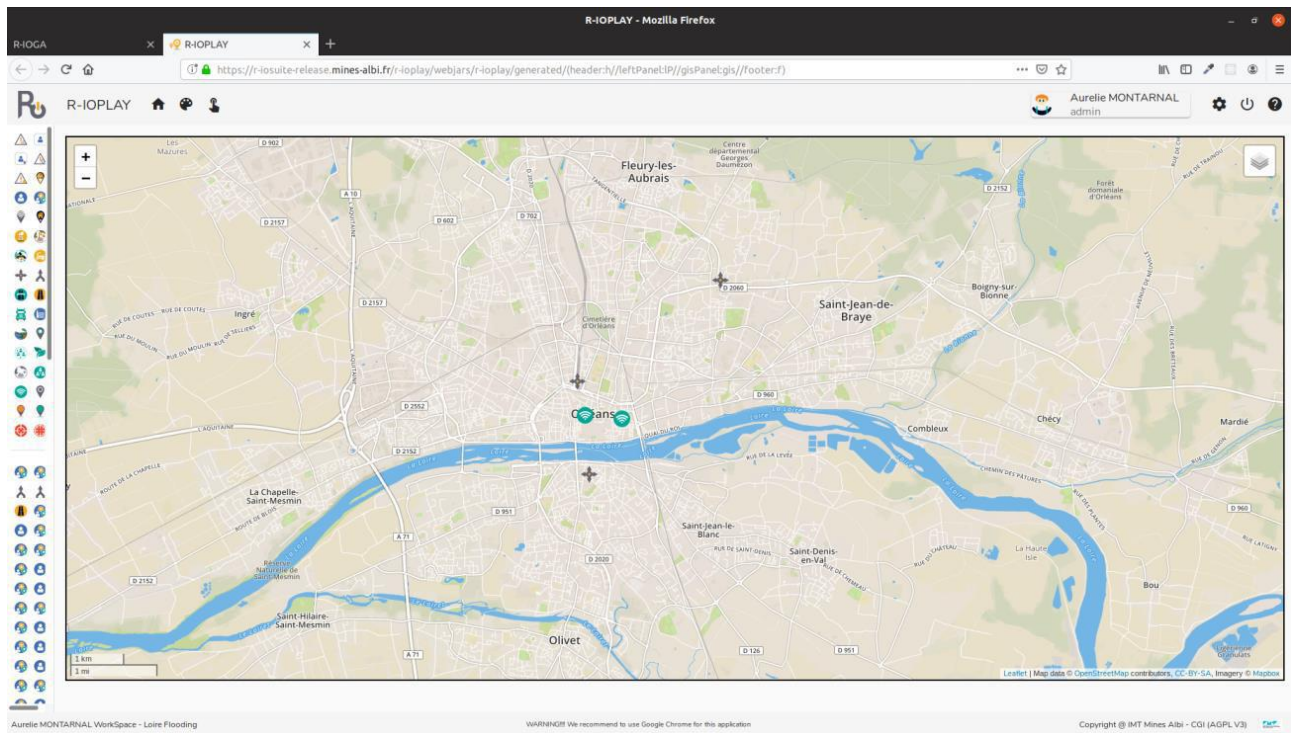


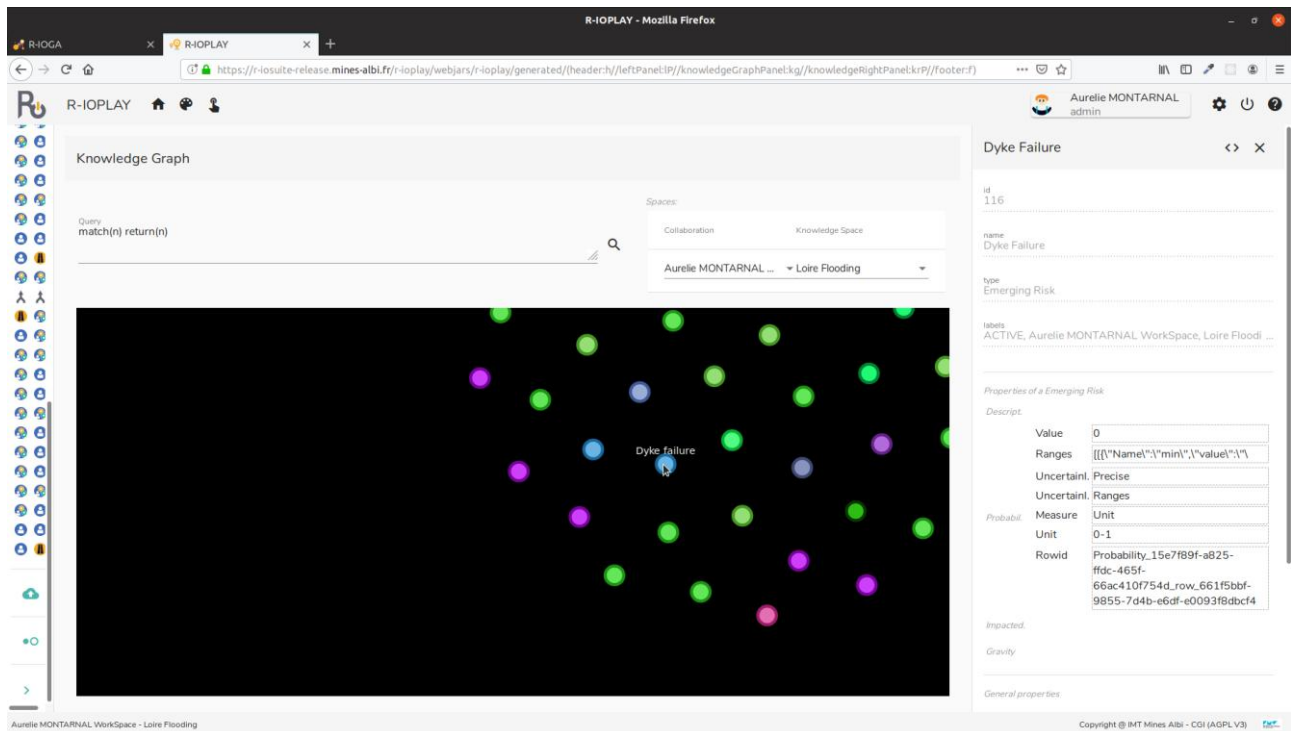
Figure A5.21: Initial state of the IO-DA GIS

```

1  <?xml version="1.0" encoding="UTF-8"?><alert xmlns:xsd="
   http://www.w3.org/2001/XMLSchema" xmlns:xsi="
   http://www.w3.org/2001/XMLSchema-instance" xmlns="
   urn:oasis:names:tc:emergency:cap:1.2">
2    <identifier>8bfcac19-cd35-48f3-9f41-4819d08ce070</identifier>
3    <sender>FRQ_COP</sender>
4    <sent>2017-03-06T14:28:43+01:00</sent>
5    <status>Exercice</status>
6    <msgType>Alert</msgType>
7    <scope>Restricted</scope>
8    <info>
9      <category>Infra</category>
10     <event>Dyke failure</event>
11     <urgency>Immediate</urgency>
12     <severity>Severe</severity>
13     <certainty>Observed</certainty>
14     <eventCode>
15       <valueName/>
16       <value/>
17     </eventCode>
18     <effective>2017-03-06T14:49:02+01:00</effective>
19     <senderName>FRQ OrgUnit 1</senderName>
20     <headline>FR</headline>
21     <description>FR</description>
22     <area>
23       <areaDesc>Orleans</areaDesc>
24       <polygon>47.897041, 1.904154, 47.897013, 1.90557, 47.89661,
25         1.90557, 47.896696, 1.904454, 47.897041, 1.904154</polygon>
26     </area>
27 </info>
</alert>

```

Figure A5.22: CAP message sent to the Test-bed and received by IO-DA



**Figure A5.23: The data has been successfully integrated into the knowledge base**

#### TR #1b – Visualization of data

1. IO-DA's database is successfully completed thanks to the previous test.
2. From this database, IO-DA successfully completed the GIS representation so that it would show the new information (see Figure A5.18).

#### TR #2a – Decision help

1. From IO-DA's database, a BPMN process was successfully generated to solve the crisis (see Figure A5.19).
2. This process is successfully converted into a JSON file.
3. This JSON file is successfully sent to the Test-bed (see Figure A5.24 and Figure A5.25).

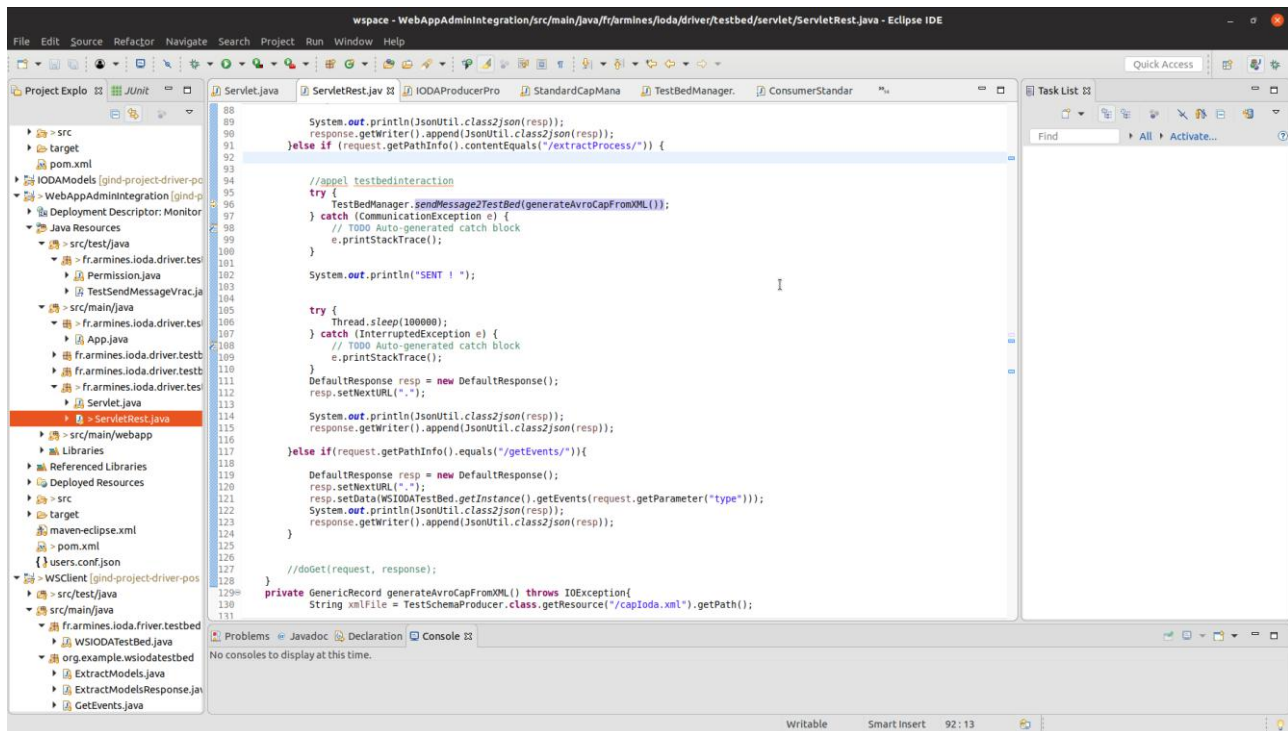


Figure A5.24: Screenshot of the method called to send process to the Test-bed

```

sasl.login.refresh.min.period.seconds = 60
sasl.login.refresh.window.factor = 0.8
sasl.login.refresh.window.jitter = 0.05
sasl.mechanism = GSSAPI
security.protocol = PLAINTEXT
send.buffer.bytes = 131072
session.timeout.ms = 10000
ssl.cipher.suites = null
ssl.enabled.protocols = [TLSv1.2, TLSv1.1, TLSv1]
ssl.endpoint.identification.algorithm = https
ssl.key.password = null
ssl.keymanager.algorithm = SunX509
ssl.keystore.location = null
ssl.keystore.password = null
ssl.keystore.type = JKS
ssl.protocol = TLS
ssl.provider = null
ssl.secure.random.implementation = null
ssl.trustmanager.algorithm = PKIX
ssl.truststore.location = null
ssl.truststore.password = null
ssl.truststore.type = JKS
value.deserializer = class to.confluent.kafka.serializers.KafkaAvroDeserializer

2019-08-07 15:18:04 INFO KafkaAvroDeserializerConfig:175 - KafkaAvroDeserializerConfig values:
  schema.registry.url = [http://tb2.driver-testbed.eu:3522]
  auto.register.schemas = true
  max.schemas.per.subject = 1000
  specific.avro.reader = false

2019-08-07 15:18:04 INFO KafkaAvroDeserializerConfig:175 - KafkaAvroDeserializerConfig values:
  schema.registry.url = [http://tb2.driver-testbed.eu:3522]
  auto.register.schemas = true
  max.schemas.per.subject = 1000
  specific.avro.reader = false

2019-08-07 15:18:04 INFO AppInfoParser:109 - Kafka version : 2.0.0
2019-08-07 15:18:04 INFO AppInfoParser:110 - Kafka commitId : 3462a8361b734732
2019-08-07 15:18:04 INFO CISAAdapter:272 - New Generic Callback Consumer created for topic: system_tuning_control
2019-08-07 15:18:04 INFO CISAAdapter:272 - InitializeProducers -->
2019-08-07 15:18:04 INFO Metadata:273 - Cluster ID: uG8vBuUvY-vzGUBLz_rug
2019-08-07 15:18:04 INFO AbstractCoordinator:677 - [Consumer clientId=consumer-3, groupId=test_new] Discovered group coordinator tb2.driver-testbed.eu:3521 (id: 2147483646 rack: null)
2019-08-07 15:18:04 INFO ConsumerCoordinator:462 - [Consumer clientId=consumer-3, groupId=test_new] Revoking previously assigned partitions []
2019-08-07 15:18:04 INFO ConsumerCoordinator:509 - [Consumer clientId=consumer-3, groupId=test_new] (Re-)joining group
SENT !
2019-08-07 15:18:08 INFO AbstractCoordinator:473 - [Consumer clientId=consumer-2, groupId=test_new] Successfully joined group with generation 8
2019-08-07 15:18:08 INFO AbstractCoordinator:473 - [Consumer clientId=consumer-1, groupId=test_new] Successfully joined group with generation 8
2019-08-07 15:18:08 INFO AbstractCoordinator:473 - [Consumer clientId=consumer-3, groupId=test_new] Successfully joined group with generation 8
2019-08-07 15:18:08 INFO ConsumerCoordinator:280 - [Consumer clientId=consumer-3, groupId=test_new] Setting newly assigned partitions [system_tuning_control-0]
2019-08-07 15:18:08 INFO ConsumerCoordinator:280 - [Consumer clientId=consumer-2, groupId=test_new] Setting newly assigned partitions [system_topic_access_invite-0]
2019-08-07 15:18:08 INFO ConsumerCoordinator:280 - [Consumer clientId=consumer-1, groupId=test_new] Setting newly assigned partitions [system_admin_heartbeat-0]

```

Figure A5.25: file successfully sent to the Test-bed

## A5.4 PROCEED Laboratory

Use Cases and Test Scenario for the PROCEED Laboratory solution are presented in section 6.3.5. This annex presents the corresponding test report.

Before executing this test a PROCEED Laboratory application is set up and the connection to the Test-bed is initialised. Then the steps described in the following sections were executed.

PROCEED Laboratory administrator: Radosław Bojba.

### TR #1 – Distribution of objects' attributes

1. The PROCEED Laboratory operator successfully logs in to PROCEED Laboratory and successfully selects an exemplary scenario.
2. The PFSP is transmitted to the Test-bed broker after the PROCEED Laboratory operator clicks on the "EXPORT" button.
3. A tester observes a set of received messages in the Test-bed broker monitor. All messages have a correct syntax. The received information is compliant with the objects' configuration in PROCEED Laboratory.

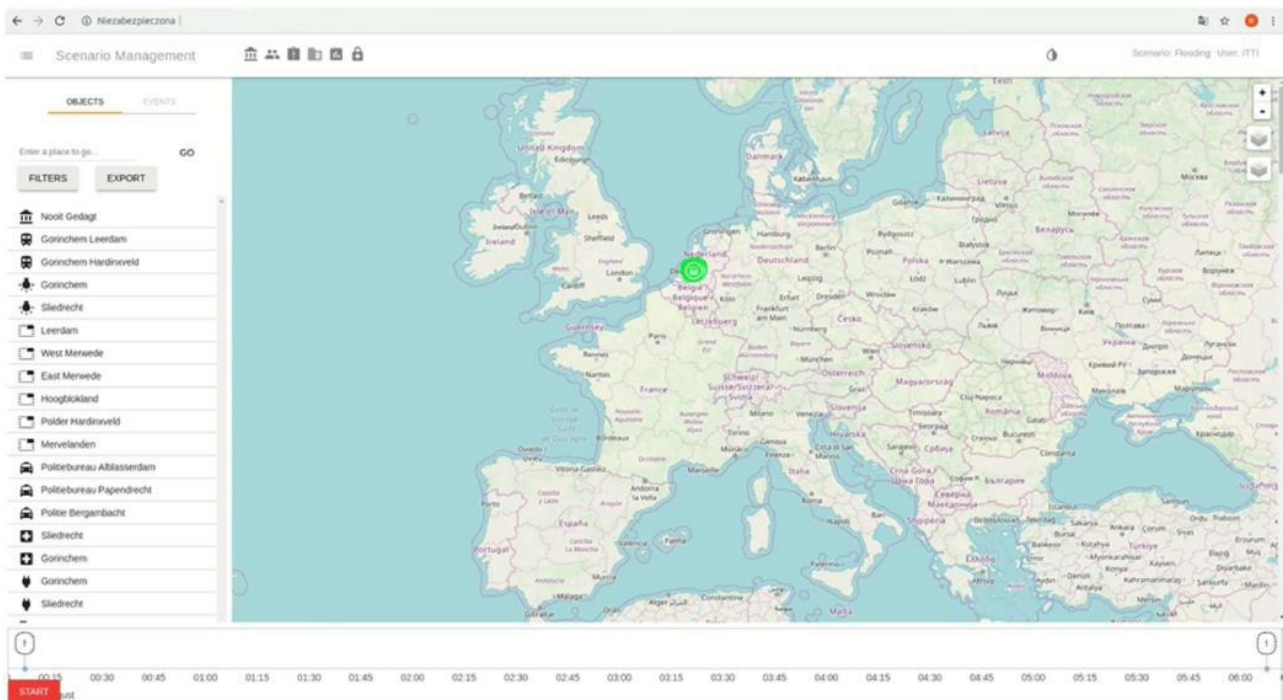


Figure A5.26: PROCEED Laboratory screen – exporting objects



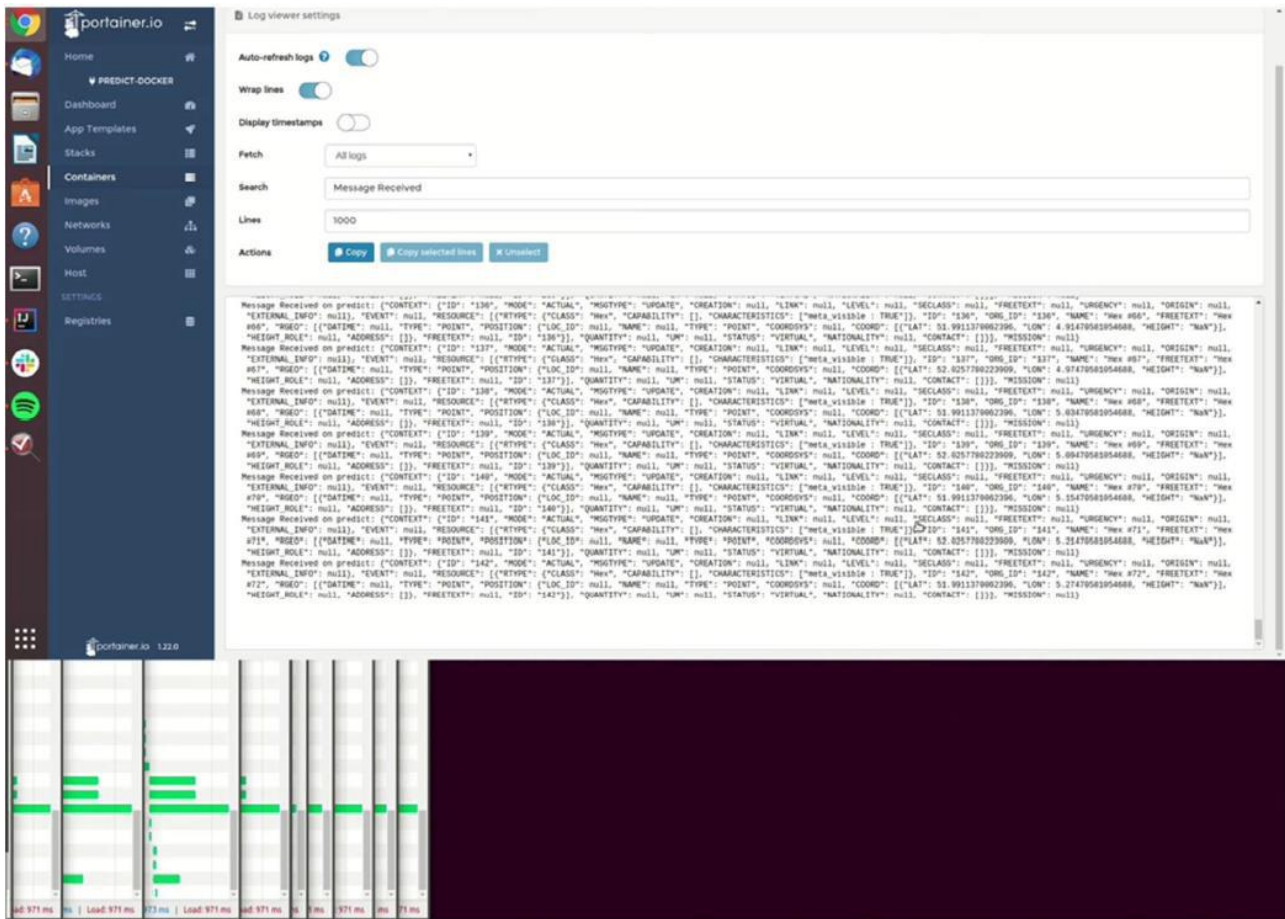


Figure A5.27: PFSP received by the Test-bed broker

The test run has been documented in the form of screen grabbed video.

## Annex 6 – Sample safety and security norms for pertinent “Technology-Impact” combinations

Selected regulations on safety and security of Crisis Management solutions are presented in the table below.

Although in no way is this table comprehensive, it intentionally includes a broad variety of sources, such as international (ISO) and European standards, national standards, potential standards /under development/, i.e. CEN Workshop Agreements (CWAs), EU Directives, regulations, recommendations and guidelines by UN bodies such as ITU and IAEA, good practices identified by industry associations and non-governmental organisations, etc.

A number of these norms are relevant to more than one “Technology-Impact” combination. Such norms are listed ones, with the respective remark on applicability.

Of general relevance is how testing fits into the development of a strategic Crisis Management capability, addressed in CEN/TS 17091:2018 “Crisis Management - Guidance for developing a strategic capability”.

Document	Relevance
<b>(1-A) Sensors and navigation systems and networks – Physical impact</b>	
EN ISO 15367-2:2005 (WI=00123043) Lasers and laser-related equipment – Test methods for determination of the shape of a laser beam wavefront - Part 2: Shack-Hartmann sensors (ISO 15367-2:2005).	Power (energy) density distribution, widths and divergence angles of laser beams.
ANSI/ISA-92.00.01-2010 (R2015), Performance requirements for toxic gas detectors.	This standard provides minimum requirements for the construction, performance, and testing of portable, trans- portable, mobile, and stationary electrical apparatus whose purpose is for the detection, measurement and notification of toxic gas in air that are used to enhance the safety of personnel in commercial and industrial locations.
ANSI/ISA-60079-0 (12.00.01)-2013 Explosive atmospheres - Part 0: Equipment - General requirements.	This standard specifies the general requirements for construction, testing and marking of electrical equipment and Ex Components intended for use in explosive atmospheres.
BS EN 50270 Electromagnetic compatibility - Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen.	This document applies to apparatus intended for use in variety of settings, including hazardous areas which could contain explosive or potentially explosive atmospheres. It specifies requirements for immunity tests in relation to continuous and transient, conducted and radiated disturbances, including electrostatic discharges, and also for emission tests.

Document	Relevance
ANSI/ISA-92.04.01, Part I-2007 (R2013) Performance requirements for instruments used to detect oxygen-deficient/oxygen-enriched atmospheres.	This standard addresses the details of construction, performance, and testing of portable, mobile, and stationary electrical instruments used to provide a warning of the presence of oxygen-deficient or oxygen-enriched atmospheres.
Radiation protection of the public and the environment, IAEA safety standards series No. GSG-8 [applicable to 1-G].	This safety guide provides guidance on the implementation of the requirements in the International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, in relation to protection of the public and the environment against radiation risks. It provides generic guidance on the application of the radiation protection principles of justification, of optimization of protection and safety, and of dose limits. The publication covers the protection of the public and the environment in all exposure situations, including in emergency.
<b>(1-B) Sensors and navigation systems and networks – Psychological impact, impact on perceptions</b>	
ISO 27048:2011 Radiation protection — Dose assessment for the monitoring of workers for internal radiation exposure.	This standard specifies the minimum requirements for the evaluation of data from the monitoring of those occupationally exposed to the risk of internal contamination by radioactive substances. It presents procedures and assumptions for the standardised interpretation of monitoring data, in order to achieve acceptable levels of reliability. Among others, it addresses assumptions for the selection of dose-critical parameter values; criteria for determining the significance of monitoring results; their interpretation; uncertainties arising from sampling, measurement techniques and working conditions; interpretation of multiple data arising from different measurement methods at different times, handling data below the decision threshold, rogue data.
<b>(1-G) Sensors and navigation systems and networks – Environmental impact</b>	
Guide for the selection of explosives detection and blast mitigation equipment for emergency, First Responders Preparedness Directorate, Office of Grants and Training, Guide 105–07, US Department of Homeland Security, February 2008 [applicable to 1-A, 8-A, 8-D, 8-F].	The guide presents a broad spectrum of sensing technologies and techniques, with their advantages and disadvantages, of visual detection and blast mitigation equipment, as well as methods and results of the evaluation of concrete products.



Document	Relevance
CEN/TS 17021:2017 Stationary source emissions - Determination of the mass concentration of sulphur dioxide by instrumental techniques [applicable to 1-A].	This technical specification describes a method, based on instrumental techniques, for sampling and determining the concentration of gaseous sulphur dioxide (SO <sub>2</sub> ) emissions from stacks. It is applicable to both periodic measurements and the calibration of automated measuring systems.
<b>(2-A) Communications – Physical impact</b>	
Security in telecommunications and information technology: An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications (Geneva: ITU-T – Telecommunication Standardization Bureau, 2015). – 206pp. [applicable to groups 2, 3 and 4].	This manual provides a broad introduction to the ICT security work of the ITU, with key areas and a discussion of the basic requirements for the protection of ICT applications, services and information, security architectures and management. An 8-page annex provides a list of relevant ITU recommendations and standards.
Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) and repealing Directive 2004/40/EC.	This directive lays down minimum requirements for the protection of workers from risks to their health and safety arising, or likely to arise, from exposure to electromagnetic fields during their work. It covers all known direct and indirect biophysical effects caused by electromagnetic fields and provides exposure limit values (ELVs) with scientifically well-established links between short-term direct biophysical effects and exposure to electromagnetic fields.
<b>(2-B) Communications – Psychological Impact, impact on perceptions</b>	
ISO 22322:2015: Societal security — Emergency management — Guidelines for public warning [applicable to 2-A, 2-F, 2-G].	This international standard provides guidelines for developing, managing, and implementing public warning before, during, and after incidents.
<b>(2-C) Communications – Personal Data</b>	
Safety, privacy and security across the mobile ecosystem: Key issues and policy implications (London: GSMA, no date). [applicable to 2-B and 2-E].	The document provides guidelines for protecting users of mobile communications devices and their privacy, and providing public safety, device integrity and protection of network security.
<b>(2-E) Communications – CIA of Information</b>	
ETSI/TS 119 312 Electronic signatures and infrastructures (ESI); Cryptographic suites.	The technical specifications provide guidance on selection of cryptographic suites with particular emphasis on interoperability. The present document is based on the specified agreed cryptographic mechanisms of the SOG-IS

Document	Relevance
	Crypto Evaluation Scheme. The SOG-IS Crypto WG is in charge of providing requirements and evaluation procedures related to cryptographic aspects of Common Criteria security evaluations of IT products.
IEEE 802.11i-2004.	An amendment to the original IEEE 802.11, implemented as Wi-Fi Protected Access II (WPA2), this standard specifies security mechanisms for wireless networks.
Sheila Frankel, Bernard Eydt, Les Owens, and Karen Scarfone, <i>Establishing wireless robust security networks: A guide to IEEE 802.11i recommendations</i> , Special publication 800-97, NIST, 2007.	Assists the understanding, selecting, and implementing technologies, security features and capabilities associated with IEEE 802.11i through its framework for Robust Security Networks (RSN); provides extensive guidance on the planning and deployment of RSNs.
CR 14302:2002 Health informatics – Framework for security requirements for intermittently connected devices [applicable to 2-C, 3-C, 3-E].	This CEN Report aims to provide a basis for a planned European Standard on the same subject and to serve as guidance to projects using cards in health care for patients, professionals and other persons working in the health care sector. It defines a framework of security requirements in systems with intermittently connected devices
<b>(2-F) Communications – Critical infrastructures</b>	
ITU-T K.87 (06/2016) Guide for the application of electromagnetic security requirements – Overview [applicable to 2-A and 2-E, 3-E and 3-F].	This document outlines electromagnetic security risks of telecommunication equipment and illustrates how to assess and prevent those risks, in order to manage information security management systems (ISMS) in accordance with Recommendation ITU-T X.1051. Major electromagnetic security risks addressed in this recommendation are as follows: natural electromagnetic (EM) threats (e.g., lightning); unintentional interference (i.e., electromagnetic interference, EMI); intentional interference (i.e., intentional electromagnetic interference, IEMI); deliberate EM attacks; information leakage from EM emanation (i.e., electromagnetic security, EMSEC); and mitigation methods against electromagnetic security threats.
ITU-T K.81 (06/2016) High-power electromagnetic immunity guide for telecommunication systems [applicable to 2-A and 2-E, 3-E and 3-F].	The document presents guidance on establishing the threat level presented by an intentional HPEM attack, the physical security measures that may be used to minimize this threat, and provides information on the vulnerability of equipment. The equipment is assumed to meet the immunity requirements presented in Recommendation ITU-T K.48 and relevant resistibility requirements.

Document	Relevance
<b>(2-G) Communications – Environmental impact</b>	
Maximum exposure levels to radiofrequency fields —3 kHz to 300 GHz, Radiation protection series publication No. 3 (Australian Radiation Protection and Nuclear Safety Agency, 2002). [applicable to 2-A].	This Standard specifies fundamental limits ... that correlate most closely with the established biological effects for which protection is required. Therefore, a set of indicative levels called “reference levels” have been provided as an alternative means for determining compliance. ... This rationale does provide a broad overview of the scientific and philosophical considerations that lead to the derivation of the exposure limits.
Physicians for safe technology, environment and wildlife effects, <a href="https://mdsafetech.org/environmental-and-wildlife-effects/">https://mdsafetech.org/environmental-and-wildlife-effects/</a> .	A compilation of norms and studies of the harmful effects of radio, microwave communication and magnetic fields on wildlife and the environment.
<b>(3-B) Computer-based systems – Psychological Impact, impact on Perceptions</b>	
ISO 14915-2:2003 Software ergonomics for multimedia user interfaces - Part 2: Multimedia navigation and control.	This standard provides recommendations and requirements for the design of multimedia user interfaces with respect to the design of the organization of the content, navigation and media-control issues.
Eva Flaspöler et al., The human machine interface as an emerging risk (European Agency for Safety and Health at Work, 2010). [applicable to 4B].	The documents review the literature allowing to foresee multi-factorial risks (e.g. due to combined effects of poor ergonomic design, poor work organisation, mental and emotional demands); complexity of new technologies, new work processes and human-machine interface (HMI) leading to increased mental and emotional strain; poor ergonomic design of non-office visual display unit workplaces; and poor design of HMI (excessively complex or requiring high forces for operation).
<b>(3-C) Computer-based systems – Personal Data</b>	
European Commission, Information system security policy C(2006) 3602, Standard on access control and authentication, Brussels, 23/06/2011 [see also the GDPR Directive].	The standard covers the complete user rights and privileges life cycle management process and the responsibilities of all relevant parties; it does not cover access control at network level or physical access control.
ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.	This standard establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

Document	Relevance
<b>(3-E) Computer-based systems – CIA of Information</b>	
ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security.	The standard establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation of security properties of IT products. Parts 2 and 3 define operations for tailoring functional and assurance components.
ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation (reviewed and confirmed in 2014).	This is a companion document to ISO/IEC 15408. It defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the respective criteria and evaluation evidence.
<b>(3-F) Computer-based systems – Critical infrastructures</b>	
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (20).	This Directive lays down measures with a view to achieving a high common level of security of network and information systems, etc. To that end, this Directive lays down obligations ... ; ...; establishes security and notification requirements for operators of essential services and for digital service providers; etc.
ANSI/ISA-61511-1-2018 / IEC 61511-1:2016+AMD1:2017 CSV, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT).	This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010. It specifies the requirements for achieving functional safety, applies when devices that meets the requirements of the IEC 61508 series are integrated into an overall system in in a wide variety of industries.
CEN/TS 17261:2018 Biometric authentication for critical infrastructure access control - Requirements and evaluation.	This document addresses biometric recognition systems that are used as part of an automated access control system (AACS) to provide a second and independent authentication factor of the individual using the AACS to access secured areas of critical infrastructure. The requirements and test methods address biometric authentication for AACS that use biometrics as a second authentication factor to a token or proximity card.

Document	Relevance
<b>(4-B) Specialised software applications – psychological impact, impact on perceptions</b>	
Eva Flaspöler et al., The human machine interface as an emerging risk (European Agency for Safety and Health at Work, 2010). [applicable to 3B].	The documents review the literature allowing to foresee multi-factorial risks (e.g. due to combined effects of poor ergonomic design, poor work organisation, mental and emotional demands); complexity of new technologies, new work processes and human-machine interface (HMI) leading to increased mental and emotional strain; poor ergonomic design of non-office visual display unit workplaces; and poor design of HMI (excessively complex or requiring high forces for operation).
<b>(4-C) Specialised software applications – Personal Data</b>	
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), <i>Official Journal</i> L 119, 4 May 2016.	Defines principles relating to and lawfulness, and conditions of processing of personal data.
CEN ISO/TS 18530:2015 (WI=00251310) Health Informatics - Automatic identification and data capture marking and labelling - Subject of care and individual provider identification (ISO/TS 18530:2014).	The document outlines the standards needed to identify and label the Subject of Care (SoC) and the Individual Provider on objects such as wrist bands, identification tags or other objects, to enable automatic data capture using data carriers in the care delivery process. It is to be used in conjunction with the GS1[1] system of standards. ISO/TS 18530:2014 describes good practices to reduce/avoid variation and workarounds which challenge the efficiency at the point of care and compromise patient safety.
<b>(4-E) Specialised software applications – CIA of Information</b>	
The ISO 27000 family of standards [applicable to 3-C, 3-E, 3-F, 4-F, 9-E].	The series provides best practice recommendations on information security management—the management of information risks through information security controls—within the context of an overall Information security management system (ISMS). In particular ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

Document	Relevance
ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [applicable to 3-C, 3-E, 3-F, 4-F, 9-E].	The standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment.
<b>(4-F) Specialised software applications – Critical infrastructures</b>	
NIST Special Publication 800-53 “Security and privacy controls for federal information systems and organizations”, revision 4, April 2014 [applicable to 3-C, 3-E, 3-F, 4-F, 9-E].	The document provides a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber and other threats.
<b>(5-A) Transport vehicles and equipment – Physical impact</b>	
<b>CEN/TR 1459-6:2015</b> (WI=00150078) Rough-terrain trucks - Safety requirements and verification.	Explains the risk assessment methodology followed to determine the Performance Level required, for specific safety related parts of control system (SRP/CS) of rough-terrain variable-reach trucks. Part 6 examines the application of EN ISO 13849-1 to slewing and non-slewing variable-reach rough-terrain trucks.
ISO 26262-2:2018 Road vehicles -- Functional safety -- Part 2: Management of functional safety.	This standard is intended for application to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles.
EN 1789:2007+A2:2014 Medical vehicles and their equipment – Road ambulances.	The standard gives general requirements for medical devices carried in road ambulances and used therein and outside hospitals and clinics in situations where the ambient conditions can differ from normal indoor conditions.
EN 13718-2:2015/prA1 (WI=00239045) Air ambulances - Part 2: Operational and technical requirements for air ambulances.	This part of EN 13718 specifies the requirements for performance and equipping for air ambulances, including requirements for interfaces to medical devices used for the transport and treatment of sick or injured persons. Applicable to both helicopter and fixed wing based ambulances capable of transporting at least one person on a stretcher.
DO-178B, Software considerations in airborne systems and equipment certification (applies also to 4-A).	A guideline dealing with the safety of safety-critical software used in certain airborne systems. DO-178C is the primary document by which the certification authorities such as FAA, EASA and Transport Canada approve all commercial software-based aerospace systems.

Document	Relevance
<b>(5-D) Transport vehicles and equipment – Materiel</b>	
ISO 19116:2019 Geographic information — Positioning services [applicable to 5-A, 5-F, 6-A, 6-D, 6-F].	This document specifies the data structure and content of an interface that permits communication between position-providing device(s) and position-using device(s) enabling the position-using device(s) to obtain and unambiguously interpret position information and determine, based on a measure of the degree of reliability, whether the resulting position information meets the requirements of the intended use.
Special operations accreditation standards of the Commission on accreditation of medical transport systems, May 2018 (applies also to 5-A).	Section 02.03 provides requirements to Safety Management Systems.
<b>(5-F) Transport vehicles and equipment – Critical infrastructures</b>	
IEEE 1609.0-2013 - IEEE guide for wireless access in vehicular environments (WAVE) – Architecture [applicable to 5-A and 5-D].	This guide describes the architecture and services necessary for WAVE devices to communicate in a mobile vehicular environment, to be used in conjunction with the family of IEEE 1609 standards.
<b>(5-G) Transport vehicles and equipment – Environmental impact</b>	
Directive 2008/68/EC of the European Parliament and of the Council of 24 September 2008 on the inland transport of dangerous goods [applicable to 5-A and 5-D].	The Directive applies to the transport of dangerous goods by road, by rail or by inland waterway within or between Member States, including the activities of loading and unloading, the transfer to or from another mode of transport and the stops necessitated by the circumstances of the transport.
<b>(6-A) Remotely controlled systems and autonomous vehicles and systems – Physical impact</b>	
Jurisdictional guidelines for the safe testing and deployment of highly automated vehicles, American Association of Motor Vehicle Administrators, Vehicle Standing Committee, Autonomous Vehicles Best Practices Working Group, May 2018 [applicable 6-D and 6-F].	Recommendations for voluntary regulation of testing and deployment of highly automated vehicles. Includes administrative, vehicle credentialing (including section 4.7 on safety standards), driver licensing, and law enforcement considerations.
Ludovic Apvrille et al., Autonomous drones for disasters management: Safety and security verifications, AT-RASC 2015.	The paper presents a tool (SysML-Sec/TTool) that can be used for formally verifying the safety and security of an autonomous drone mission and flight, based on an architecture developed within drone4u project.



Document	Relevance
<b>(6-D) Remotely controlled systems and autonomous vehicles and systems – Materiel</b>	
CWA 17357:2019 Urban search and rescue (USaR) robotic platform technical and procedural interoperability – Guide [applicable to 6-A].	This CWA provides recommendations to enable interoperability between USaR robotic platforms and the equipment, sensors and tools that are attached to them; principles for enabling USaR robotic platforms to operate in all ground search environments.
NASA-STD-8719.13C, Software safety standard (2013) [applicable also to 5-D].	This standard defines the requirements to implement a systematic approach to software safety as an integral part of system safety and the overall safety program of a program, project, or facility. It specifies the software activities, data, and documentation necessary for the acquisition and development of software in a safety critical system.
<b>(6-E) Remotely controlled systems and autonomous vehicles and systems – CIA of information</b>	
PAS 1885:2018 The fundamental principles of automotive cyber security. Specification.	This PAS applies to the security and functional safety aspects of the entire automotive development and use life cycle, including specification, design, implementation, integration, verification, validation, configuration, production, operation, servicing and decommissioning. A lifecycle approach is required to tackle all the risks that will arise from a constantly changing threat landscape, so as to protect vehicles and vehicle-related systems once they have been delivered to the market.
<b>(6-F) Remotely controlled systems and autonomous vehicles and systems – Critical infrastructures</b>	
CEN - PREN 16803-2 Space – Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) – Part 2: Assessment of basic performances of GNSS-based positioning terminals [applicable to 6-A and 6-D].	This document proposes testing procedures to assess the basic performance of any GNSS-based positioning terminal for a given use case described by an operational scenario. These tests address the basic performance features Availability, Continuity, Accuracy and Integrity of the Position, Velocity and Time (PVT) information.
Guidance: The key principles of vehicle cyber security for connected and automated vehicles, Centre for the Protection of National Infrastructure, UK Department of Transport.	It is essential that all parties involved in the manufacturing supply chain are provided with a consistent set of guidelines. This Guide provides key principles for use throughout the automotive sector and its supply chain.
<b>(7-A) Fire extinguishers and decontamination devices and substances – Physical Impact</b>	
ISO 7165:2017 Firefighting -- Portable fire extinguishers -- Performance and construction.	The standard specifies the principal requirements intended to ensure the safety, reliability and performance of portable fire extinguishers; application can be extended to extinguishers having a total mass of up to 25 kg when fully charged.

Document	Relevance
EN 3-10:2009 Portable fire extinguishers. Provisions for evaluating the conformity of a portable fire extinguisher to EN 3-7 (characteristics, performance requirements and test methods).	European standard EN 3 specifies requirements for portable fire extinguishers. Compliance with the standard is legally required in the EU.
CEN/TR 15276-1:2009 Fixed firefighting systems - Condensed aerosol extinguishing systems - Part 1: Requirements and test methods for components; CEN/TR 15276-2:2009 – Part 2: Design, installation and maintenance.	This document specifies requirements and describes test methods for condensed aerosol extinguishing components, precaution requirements, e.g. that the room is evacuated and sealed off whenever a generator is activated, evacuation of the proximity area, criteria for re-entering and other safeguards as stated in Clause 5 of CEN/TR 15276-2:2009.
Guide for the selection of chemical, biological, radiological, and nuclear decontamination equipment for emergency first responders, Guide 103–06, March 2007, 2nd Edition, U.S. Department of Homeland Security.	General requirements to decontamination equipment, including delivery systems, containment devices and accessories, shelters, showers, commercial decontaminants (foams, solutions, gaseous, nonaqueous, etc.), and decontamination systems and trailers.
New rules for hazardous substances (Changes to the regulations for hazardous substances in the workplace), New Zealand Government, November 2017. [applicable also to 7-G].	Used in combination with a Practical Guide to working safely with hazardous substances, providing practical examples and definitions of key controls and terminology, and an Emergency Response Flipchart, <a href="http://www.hazardoussubstances.govt.nz">www.hazardoussubstances.govt.nz</a> .
<b>(7-D) Fire extinguishers and decontamination devices and substances – Materiel</b>	
Chemical, biological, radiological, and nuclear response, Joint Publication 3-41 (Washington, D.C.: Joint Chiefs of Staff, 9 September 2016). [applicable to the whole group 7].	Comprehensive treatment of organisational and procedural issues; includes information that can be used in designing test scenarios.
Phillip Carson and Clive Mumford, Hazardous chemicals handbook, Second edition (Oxford: Butterworth Heinemann, 2002). – 619pp. [applicable to the whole group 7].	The Handbook presents a variety of hazardous chemicals, including radioactive chemicals, safety by design principles, operating procedures, transport, impact on the environment, monitoring and protection. It includes selected topics of testing and evaluation.

Document	Relevance
<b>(7-F) Fire extinguishers and decontamination devices and substances – Critical infrastructures</b>	
CEN/TS 16595:2013 CBRN – Vulnerability assessment and protection of people at risk [applicable also to 7-A, 7-D, 7, 7-G].	This Technical Specification is based on an all-hazards approach, with a specific focus on terrorism and other security related risks. Looking at the combination of threats, vulnerabilities and values to be protected, threats may be terrorist attacks with chemical, explosive and biological agents, or nuclear waste materials, or with conventional means on CBRN plants, causing a similar devastating effect on a potentially large scale. It can serve to guide the development of safety and security test cases.
<b>(7-G) Fire extinguishers and decontamination devices and substances – Environmental impact</b>	
Guide for the selection of chemical, biological, radiological, and nuclear decontamination equipment for emergency first responders, Guide 103–06, March 2007, 2nd Edition, U.S. Department of Homeland Security [applicable to 7-A and 7-D].	General requirements to decontamination equipment, including delivery systems, containment devices and accessories, shelters, showers, commercial decontaminants (foams, solutions, gaseous, nonaqueous, etc.), and decontamination systems and trailers.
<b>(8-A) Specialised disaster management equipment – Physical Impact</b>	
Group of standards ISO 13.340 Protective equipment.	The group includes standards for protective equipment in general, protective clothing, head protective equipment (helmets, eye-protectors, hearing protectors, ear muffs, teeth protectors and hoods), respiratory protective devices, hand and arm, leg and foot protection, etc.
PD CEN/TR 14560:2018 Guidance for selection, use, care and maintenance of protective clothing against heat and flame.	This document is not exhaustive in addressing all the safety concerns associated with the use of compliant protective equipment for protection against heat and flames and other related risks. It is meant for end users, incl. those from relevant industries, fire fighters and emergency response, that may be confronted with heat and flame risks.
BS EN 943-2:2019 Protective clothing against dangerous solid, liquid and gaseous chemicals, including liquid and solid aerosols. Performance requirements for Type 1 (gas-tight) chemical protective suits for emergency teams.	This document specifies the minimum requirements, test methods, marking and information supplied by the manufacturer, for ventilated and non-ventilated gas-tight chemical protective suits for use by emergency teams.

Document	Relevance
BS EN 1073-1:2016+A1:2018 Protective clothing against solid airborne particles including radioactive contamination: Requirements and test methods for compressed air line ventilated protective clothing, protecting the body and the respiratory tract	This standard specifies the requirements and test methods for protective clothing, ventilated by an independent supply of air from an uncontaminated source, protecting the body and the respiratory system of the wearer against solid airborne particles including radioactive contamination. This kind of protective clothing can be provided with an emergency breathing facility.
ISO 15027-2:2012 Immersion suits — Part 2: Abandonment suits, requirements including safety See also ISO 15027-3 specifying test methods.	This standard specifies performance and safety requirements for abandonment suits in emergency situations in work and leisure activities to protect the body of a user against the effects of cold water immersion, such as cold shock and hypothermia, including head, hand and feet protection.
CEN/TR 16705:2014 (WI=00388001) Perimeter protection – Performance classification methodology.	This CEN Technical Report describes a performance classification methodology for the identification of the desired systems performance for perimeter protection systems. It also gives a conceptual framework for matching the desired performance and the capabilities of a possible solution.
IEC 60601-1 - Medical electrical equipment - Part 1: General requirements for basic safety and essential performance.	A series of technical standards for the safety and essential performance of medical electrical equipment. Collateral standards (numbered 60601-1-X) define the requirements for certain aspects of safety and performance, e.g. Electromagnetic Compatibility (IEC 60601-1-2). Particular standards (numbered 60601-2-X) define the requirements for specific products or specific measurements built into products.
BS EN 12931:2015 Chemicals used for treatment of water intended for human consumption. Chemicals for emergency use. Sodium dichloroisocyanurate, anhydrous See also EN 12932:2015 and EN 12933:2015.	This European Standard is applicable to sodium dichloroisocyanurate anhydrous used for emergency treatment of water intended for human consumption. It describes the characteristics of sodium dichloroisocyanurate anhydrous and specifies the requirements and the corresponding test methods for sodium dichloroisocyanurate anhydrous. It gives information on its use in water treatment. It also determines the rules relating to safe handling and use of sodium dichloroisocyanurate anhydrous.

Document	Relevance
<b>(8-C) Specialised disaster management equipment – Personal data</b>	
CEN/TR 16670:2014 Information technology – RFID (Radio-Frequency IDentification) threat and vulnerability analysis. See also CEN/TR 16674:2014 – Analysis of privacy impact assessment methodologies relevant to RFID.	This Technical Report considers the threats, vulnerabilities and mitigation methods associated with specific characteristics of RFID technology in a system. In particular the document should be a tool used by RFID system integrators, to improve security aspects using privacy by design approach.
CEN/TS 16921:2016 Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems.	This Technical Specification focuses on biometric aspects of portable verification and identification systems for law enforcement and border control authorities, balancing the needs of security, ease of access and data protection and accounting for EU privacy and data protection regulation (Directive 95/46/EC and European databases access).
<b>(8-D) Specialised disaster management equipment – Materiel</b>	
ISO/IEC 29197:2015 Information technology — Evaluation methodology for environmental influence in biometric system performance.	This standard elaborates fundamental requirements for planning and execution of environmental performance evaluations for biometric systems based on scenario and operational test methodologies, respective specifications, baseline performance and procedures for carrying out the overall evaluation.
CEN/TS 16920:2016 Environmental influence testing methodology for operational deployments of European ABC (automated border control) systems.	This document specifies the ISO/IEC 29197 testing methodology for European ABC systems, covering environmental conditions which influence biometric modalities used for European ABC systems, i.e. temperature, humidity, illumination and noise.
CEN/TS 16850:2015 Societal and citizen security – Guidance for managing security in healthcare facilities [applicable to 8-A].	The standard will specify requirements for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented security management system in healthcare facilities.
CEN/TS 17159:2018 Societal and citizen security - Guidance for the security of hazardous materials (CBRNE) in healthcare facilities [applicable to 8-A].	This Technical Specification provides guidance for managing security of (high risk) chemical, biological, radioactive, nuclear or Explosive materials, such as those covered by the EU CBRN action plan, that are used within healthcare facilities (HCF); it covers the lifecycle of such materials within a HCF's span of control. In this Technical Specification these materials are referred to as "CBRNE materials". It applies to circumstances where healthcare is provided at locations remote from the normal location of the HCF.

Document	Relevance
Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC See also Commission Implementing Decision (EU) 2019/436 of 18 March 2019 on the harmonised standards for machinery drafted in support of Directive 2006/42/EC [applicable to 8-A].	Annex 1 defines essential health and safety requirements relating to the design and construction of machinery, incl. ensuring that risk assessment is carried out and results are taken into account in the design and construction.
EN 981:1996+A1:2008 Safety of machinery - System of auditory and visual danger and information signals [applicable to 8-A].	A system of danger and information signals is specified taking into account the different degrees of urgency.
<b>(8-E) Specialised disaster management equipment – CIA of Information</b>	
CEN/TS 15291:2006 Identification card system – Guidance on design for accessible card-activated devices [applicable to 8-A, 8-D and 8-F].	This document provides guidance for the design and location of card-activated devices and the immediate environment, to facilitate access for the widest possible range of users (all/most members of the community), subject to conditions of adequate privacy and security.
<b>(8-F) Specialised disaster management equipment – Critical infrastructures</b>	
B. Wisner and J. Adams, eds., Environmental health in emergencies and disasters: A practical guide, World Health Organization 2002. [applicable to 8-A and 8-G].	The document provides guidelines for shelter and emergency settlements, water supply, sanitation, food safety, vector and pest control, control of communicable diseases and prevention of epidemics, chemical incidents, radiation emergencies, etc.
CWA 17260:2018 Guidelines on evaluation systems and schemes for physical security products [applicable to 8-A and 8-D].	This CWA provides guidelines on how to design certification systems and schemes for physical security products and presents a framework in which these systems and schemes can be upheld. Physical security products include products which provide protection of people, property and infrastructure from acts of malicious intent, such as physical attacks.
CEN/TS 13763-27:2003 Explosives for civil uses - Detonators and relays Part 27: Definitions, methods and requirements for electronic initiation systems [applicable to 8-A and 8-D].	This Technical Specification specifies a risk analysis, evaluation and testing procedure to be used to investigate the safety and reliability of electronic initiation systems by identifying hazards and estimating the risks associated with the system. The Technical Specification also stipulates levels of acceptability for electronic initiation systems.

Document	Relevance
<b>(8-G) Specialised disaster management equipment – Environmental impact</b>	
Group of ISO standards 13.030.30 Special wastes, including radioactive wastes, hospital wastes, carcasses, electrical, electronic equipment and other hazardous wastes.	See ISO/DIS 16640 Monitoring radioactive gases in effluents from facilities producing positron emitting radionuclides and radiopharmaceuticals; ISO/DIS 22450 Elements recycling – Communication formats for providing recycling information on rare earth elements in industrial waste and end of life products; etc.
Group of ISO standards 13.030.20 Liquid wastes. Sludge.	Requirements to sludge recovery, recycling, treatment and disposal, e.g. Guidance on thermal treatment (ISO/DTR 20736); Beneficial use of biosolids — Land applications (ISO/DIS 19698); etc.
IAEA Regulations for the safe transport of radioactive material, 2018 edition, No. SSR-6(Rev.1).	The Regulations establish standards of safety which provide an acceptable level of control of the radiation, criticality and thermal hazards to people, property and the environment that are associated with the transport of radioactive material. It is supplemented by a hierarchy of Safety Guides (applicable also to 8-A and 8-D).
CEN/TR 16928:2016 Guidance for the implementation of environmental aspects in product standards and system standards in the field of wastewater engineering	This document applies for the implementation of environmental aspects in product standards and system standards in the field of wastewater engineering. It provides a structure on how to identify and consider environmental aspects and potential environmental impacts of products and systems in the field of wastewater engineering throughout their life cycle.
<b>(9-A) Training and personnel services – Physical impact</b>	
ISO 22398:2013 – Societal security — Guidelines for exercises.	This International Standard describes the elements of a generic approach to planning, conducting and improving exercise programmes and projects. It introduces the “exercise safety officer” position for a person tasked with ensuring that any actions during the exercise are performed safely.
Guidelines for first responders to a CBRN incident, Project on minimum standards and non-binding guidelines for first responders regarding planning, training, procedure and equipment for CBRN incidents, NATO Civil Emergency Planning Civil Protection Group, updated 01/08/2014.	The response guidelines are generic in nature and relate to procedures, capabilities and equipment required to implement an effective response.



Document	Relevance
Methodological guide on safety exercises in road tunnels (Bron, France: Centre d'Études des Tunnels, June 2017).	The document presents the regulatory context and good practices in organising exercise involving various stakeholders. It includes guidance on conducting technical tests on safety equipment.
<b>(9-B) Training and personnel services – Psychological impact, impact on Perceptions</b>	
Robert Macpherson, Safety & security handbook, CARE International, no date. [applicable to 9-A].	The Handbook provides guidance for policies and procedures for personal safety and security, behaviour in the face of hazards and various incidents, and on stress management.
IASC Guidelines on mental health and psychosocial support in emergency settings (Geneva: Inter-Agency Standing Committee, 2007 & 2008).	The Guidelines present good practice in planning, establishing and coordinating a set of minimum multi-sectoral responses to protect and improve people's mental health and psychosocial well-being in the midst of an emergency. The 2008 edition provides a Checklist for Field Use.
<b>(9-C) Training and personnel services – Personal data</b>	
Guide to the general data protection regulation (GDPR), ver. 1.0.248 (Information Commissioner's Office, August 2018). [See also the GDPR Directive].	The Guide explains the provisions of the GDPR to help organisations comply with its requirements. It is intended for those who have day-to-day responsibility for data protection.
<b>(9-E) Training and personnel services – CIA of Information</b>	
[See the ISO 27000 series and NIST 800-53].	
Edgar R. Weippl, Security in e-learning (Springer, 2005).	A comprehensive treatment of roles, threats, risk analysis and security controls.

## Annex 7 – Illustrative test cases

---

This Annex outlines three illustrative test cases for testing safety and security of Crisis Management solutions that have already participated in project Trials:

- The Social Media Analysis Platform, trialled in Trial France.
- The CrisisSuite solution, trialled in Trials France and The Netherlands, and in the Final Demo.
- The Test-bed infrastructure with the Common Information Space and its embedded security features.

The role and the guidelines for preparing test cases are described in DRIVER+ deliverable **D934.21 – Solution Testing Procedure** (6).

### Test Case 1 “Personal Data Protection in the Social Media Analysis Platform”

---

The Social Media Analysis Platform is presented in the DRIVER+ Portfolio of Solutions at <https://pos.driver-project.eu/en/PoS/solutions/62>.

This test case illustrates the couple 4-C (see Table 7.1), i.e. the potential negative impact of specialised software applications on personal data.

General norms: Regulation (EU) 2016/679.

Specific norms: OASIS / Common Alerting Protocol Version 1.2.

During Trial 2, the Social Media Analysis Platform (SMAP) solution was identified as requiring a GDPR analysis. The solution collects and exploits Social Media posts which are considered as “personal data.” The analysis which was conducted with the support of Thales Legal Department is reproduced in the Annex 2 of **D942.22 Report on the application of solutions in the Trial 2**. In short, this analysis concluded that due to the fact that the purpose of the collection and processing of these personal data was clearly aiming at improving Social Resilience, and thus was in the interest of the persons, they were legitimate, and consequently authorized. Yet, due to the specific nature of the data, some restrictions regarding the access to the data needed to be limited (through authentication of a single user) and their retention over time also. In addition to these measures, the anonymization of the pseudonyms (which often contain names in clear) was recommended and implemented. This analysis is a good basis to foresee the requirements which could derive for such a Social Media Analysis Platform if it were to become an operational system.

### Test Case 2 “Providing confidentiality, integrity and availability of information in CrisisSuite”

---

The CrisisSuite solution is presented in the DRIVER+ Portfolio of Solutions at <https://pos.driver-project.eu/en/PoS/solutions/22>.

This test case illustrates the couple 4-E (see Table 7.1), i.e. the potential negative impact of using specialised software applications to exchange information among units participating in a Crisis Management operation on its confidentiality, integrity and availability.

General norms: The ISO 27000 family of standards.

The CrisisSuite solution was trialled three times during DRIVER+ - in two Trials and the Final Demonstration. The example which is the most meaningful with regards to the requirements concerning safety and security is the one of the Final Demonstration. In that demonstration, information was shared thanks to CrisisSuite which is deployed at three levels, from EUCPM modules (the tactical level), then at EUCPT level (the operational coordination level), and ERCC, the strategic coordination at European level. The security problems which were faced during the Final Demonstration related to the right to know (confidentiality) of information: ERCC does not want modules to be able to read the information they share with EUCPT.

During the Final Demonstration, this requirement was implemented by creating two “crises” in CrisisSuite. This implementation was a work around which actually was satisfying for the table top Trial, but would require other types of implementation if the solution was to be operationally deployed at ERCC, EUCPT and Modules.

### Test Case 3 “Security of digital infrastructure in the Common Information Space”

---

The Test-bed technical infrastructure is presented in detail in the deliverables from Work Package 923 of the DRIVER+ project.

This test case illustrates the couple 3-E (see Table 7.1), i.e. the potential negative impact of computer-based systems on critical infrastructures; in this case – on the digital infrastructure of a Crisis Management operation. Although the illustration relates to Trial settings, the approach can be of value in testing actual digital infrastructure.

General norms: The ISO 27000 family of standards.

Specific norms: SSL/TLS security protocol.

The Common Information Space (CIS) is a software module of the Test-bed infrastructure which enables the exchange of information between solutions in DRIVER+ Trials. This CIS can be made available on-line which facilitates on-line testing of solutions or the use of the on-line Test-bed during a Trial. Making such software available on-line makes it vulnerable to potential cyber intentional attacks or non-intentional interference. A solution that would connect to an instance of the CIS during a Trial either by mistake or malicious intention could disturb the whole Trial by sending unintended messages for example. For this reason, it is very important to fully master what solution is able to connect to the CIS and when. In DRIVER+ this level of security was introduced by distributing security certificates which enforced a strong authentication mechanism on the CIS by encrypted security codes: each solution (of each organization) is issued a security certificate by a Certificate Authority of the Test-bed, and the CIS broker requires every connecting solution to authenticate with such certificate (SSL/TLS protocol). This guarantees that the solutions connecting to the CIS are indeed properly identified and authorized to do so.

Besides, the use of SSL/TLS security protocol on the CIS broker also guarantees the confidentiality and integrity of the messages exchanged within the CIS, i.e. it prevents an unauthorized user to intercept, alter, replace or replay messages maliciously. The next security requirement addressed in DRIVER+ is topic-based access control. Indeed, depending on the sensitivity or criticality of certain CIS topics, only one or more specific solutions should be authorized to publish or read data from these topics. The previous paragraph gives a relevant example where ERCC is exchanging information with EUCPT, which could be done in a specific CIS topic, but does not want the EUCPM modules to read this information. To address this requirement, DRIVER+ provides an access control plugin for the CIS broker that allows to enforce a fine-grained access control policy (defined via the Test-bed’s Admin Tool) that consists of rules such as: permit solution X to READ/WRITE from/to topic Y (and deny such rights by default). Although this feature has not

been used yet in a Trial, it is available in the Test-bed software repository and tested by the Test-bed infrastructure staff.

In the perspective of an operational use of the CIS, other security measures would be required in order to reduce its vulnerability to potential cyberattacks: the use of one single port to connect to the internet, or the use of a proxy to hide the actual IP addresses of the CIS servers from the outside.

The full securing of the CIS would also depend on the actual physical and logical infrastructure on which the servers would be deployed: the presence of a DMZ zone, firewalls, etc., which can only be examined when all these constraints are known.