



SECURE DYNAMIC CLOUD FOR
INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY
BASED ON PAN-EUROPEAN DISASTER INVENTORY

Deliverable 3.4

Final Publication of Inventory Results

Christina Schäfer¹, Torben Sauerland¹, Jens Pottebaum¹, Christoph Amelunxen¹, Robin Marterer¹, Daniel Eisenhut¹, Christoph Schwentker¹, Michaela Brune¹, Daniel Behnke², Simona de Rosa³, Andrea Nicolai³, Ioannis Daniilidis⁴, Dimitris Kavalieros⁴, Paul Hirst⁵

¹ University of Paderborn, ² Technical University Dortmund, ³T6 ECO, ⁴KEMEA, ⁵BAPCO

February 2017

Work Package 3

Project Coordinator

Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme

for Research and Technological Development

COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems
and data set used by first responders and police authorities





Distribution level		Public		
Due date		28/02/2017		
Sent to coordinator		28/02/2017		
No. of document		D3.4		
Name		<i>Final Publication of Inventory Results</i>		
Type		<i>Report</i>		
Status & Version		1.0		
No. of pages		108		
Work package		3		
Responsible		UPB		
Further contributors		TUDO T6 ECO		
Keywords		<i>inventory results, data sets, command systems, process analysis, information systems, business models,</i>		
History	Version	Date	Author	Comment
	V0.1	01/11/2016	UPB	Draft structure
	V0.2	15/11/2016	UPB	
	V0.3	17/11/2016	UPB	
	V0.4	21/11/2016	UPB	
	V0.5	07/12/2016	UPB	Integrating internal input
	V0.6	13/01/2017	UPB, T6	Integrating input
	V0.7	16/01/2017	UPB	
	V0.8	07/02/2017	UPB, TUDO	Integrating Input
	V0.9	08/02/2017	UPB, KEMEA	Final check and integration of input from KEMEA



	V1.0	24/02/2017	UPB, ULANC, BAPCO	Integrating QA + monitoring comments
--	------	------------	----------------------	--------------------------------------

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.



Authors



University of Paderborn
C.I.K.

Christina Schäfer
Email: c.schaefer@cik.upb.de
Jens Pottebaum
Email: pottebaum@cik.upb.de
Christoph Amelunxen
Email: amelunxen@cik.upb.de
Robin Marterer
Email: Marterer@cik.upb.de
Torben Sauerland
Email: sauerlandtorben@gmail.com
Daniel Eisenhut
Email: daniel90@campus.upb.de
Christoph Schwentker
Email: cschwentker@gmail.com
Michaela Brune
Email: mbrune2@mail.uni-paderborn.de



TU Dortmund
CNI

Daniel Behnke
Email: daniel.behnke@tu-dortmund.de



T6 Ecosystems

Andrea Nicolai
Email: a.nicolai@t-6.it
Simona De Rosa
Email: s.derosa@t-6.it



Center for Security Studies
(KEMEA)
P.Kanellopoulou 4
1101 77 Athens
Greece

Ioannis Daniilidis
Email: i.daniilidis@kemea-research.gr

Dimitris Kavalieros
Email: d.kavallieros@kemea-research.gr



BAPCO

Paul Hirst
Email: paul.hirst@bapco.org.uk



Reviewers



ULANC

Katrina Petersen
Email: k.petersen@lancaster.ac.uk



BAPCO

Paul Hirst
Email: paul.hirst@bapco.org.uk

Monitoring



ULANC

Monika Büscher
Email: m.buscher@lancaster.ac.uk



Executive summary

This deliverable describes the final collection of inventory content in WP3 and is thus a continuation of the previously published D3.3. In order to give a summary of research undertaken in this work package, all chapters include a description of activities for gathering and analysing the respective inventory categories. These are data sets, command systems including information management processes, information systems, and business models. The main contributions are based on literature research and identification of already existing background in the consortium. These activities were complemented by several interactions with stakeholder groups, including co-design workshops involving the participation of external advisors to the project. Moreover, a concept and implementation as proof of concept for publishing inventory content is described in Chapter 6.

One major area of research in this work package is **data sets and further way to categorise, structure and use of data sets in emergency situations**. This Deliverable demonstrates the ongoing work on refinements and adjustments to define the final data model of SecInCoRe based on the available data-sets gathered across different types of disasters (see D2.1 and D3.1) and already existing data networks (i.e. Linked Open Data).

Another category of the inventory is **command systems including information management processes**. To demonstrate the research results of this task a three-step approach was employed. First, based on a high-level perspective, relevant organisations at the EU-level were identified that used information systems to ensure an ongoing information flow. Further, a break down on national level was conducted. Individual command and control systems were analysed and modelled to define similarities and differences. In a next step, information management processes and command processes used in practice were taken into account using the refugee crisis as an example.

Next is the section on **research and inspection of information and communication systems**. Based on the database scheme for information systems defined in the previous deliverable, a dedicated database, as one part of the Knowledge Base, was developed. The database was continuously updated to include further gathered information systems. The success of information systems is essential to understand stakeholder needs and therefore, success factors and barriers for the uptake of information systems were analysed, taking the results from the previous deliverable D3.3 into account.

The reference implementation Semantic Framework, including the semantic search functionality, explores **access to the inventory content**. For this purpose a concept was defined to provide information to first responder and police authorities. Further aconnections to various data sources was conducted, which are governed by secure access policies. All different functionalities which are part of the semantic search,



support people in retrieving and understanding content of the Knowledge Base (illustrated in chapter 6).

Chapter 7 deals with the connection and impact of WP3 research results for other work packages and the last point in this deliverable take the verification and validation of the inventory, the Knowledge Base and the search into account.



Table of contents

1	Introduction	10
1.1	Purpose of this document.....	11
1.2	Validity of this document.....	11
1.3	Relation to other documents.....	11
1.4	Contribution of this document.....	12
1.5	Target audience	13
1.6	Glossary	13
1.7	List of figures	18
1.8	Structure of the deliverable.....	19
2	Final version of data sets	20
2.1	Approach	20
2.2	Evolution of the data model	22
2.2.1	<i>Origin of the data set.....</i>	<i>22</i>
2.2.2	<i>Inclusion or contradiction to the current data model.....</i>	<i>22</i>
2.2.3	<i>Incident type.....</i>	<i>24</i>
2.2.4	<i>Reflection of the data model</i>	<i>24</i>
2.2.5	<i>Final data model</i>	<i>25</i>
2.3	Publication of Data Sets	27
3	Command systems and information management processes	30
3.1	Approach	30
3.2	High-level perspective of information management process related to emergency management.....	31
3.2.1	<i>Selection of Command and Control Systems</i>	<i>35</i>
3.2.2	<i>Information management and command and control in practice</i>	<i>38</i>
4	Research and inspection of information and communication systems.....	44
4.1	Approach	44
4.2	Structure and Acquisition of Information systems.....	45
4.3	Success factors and barriers for the uptake of information systems	49
4.3.1	<i>Definition of success factors</i>	<i>49</i>
4.3.2	<i>Interactions between basic success factors from an IS providers and IS users point of view.....</i>	<i>49</i>



5	Business models for the application of information systems	59
5.1	General approach to define business models	59
5.2	Definition of the main relevant models of business	59
5.3	Report on the Business Model Inventory	62
5.4	Analysis of existing business models.....	65
6	Access to inventory content	68
6.1	Concept Semantic Framework	68
6.1.1	<i>Overall</i>	68
6.1.2	<i>Data collection</i>	70
6.1.3	<i>Data processing</i>	71
6.1.4	<i>Quality assurance</i>	73
6.1.5	<i>Data accessing</i>	74
6.2	Implementation of the Semantic Framework	75
6.2.1	<i>Research</i>	75
6.2.2	<i>Overall Architecture</i>	77
6.2.3	<i>Data collection</i>	77
6.2.4	<i>Data processing</i>	78
6.2.5	<i>Data accessing</i>	82
7	Connections between Work packages	85
7.1	Relation between WP3 and WP2	87
7.2	Relations between WP3 and WP4	87
7.2.1	<i>Usage of inventory content to derive taxonomy</i>	87
7.2.2	<i>Support defining of semantic cloud services</i>	89
7.3	Relations between WP3 and WP5	90
7.4	Relations between WP3 and WP6	90
8	Verification and Validation of Inventory, Knowledge Base and Search	91
8.1	Inventory.....	91
8.2	Knowledge Base	95
8.3	Search	97
9	Literature index	104

1 Introduction

SecInCoRe develops a Pan-European inventory of past critical events and disasters, their consequences (especially in terms of time dimension and costs) focused on collaborative emergency operations and especially planning and preparing to emergency operations (see [4]). Moreover, the focus is on creating a critical mass of content and the infrastructure for a self-sustaining dynamic inventory that grows with the evolving landscape of first responder and police authorities' practice.

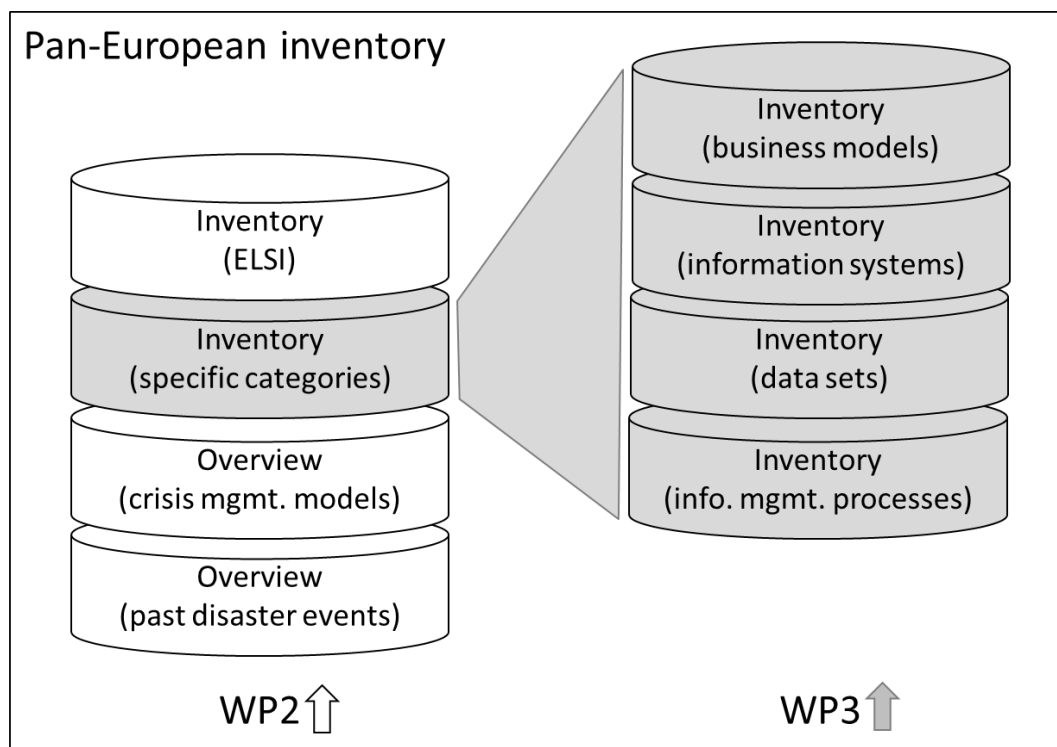


Figure 1: Inventory content

The inventory of disaster events is complemented by an inventory of related information. Following the high-level SecInCoRe objectives (see [3]) and the research methodology (WP3, see [5]) the inventory includes the following categories (see Figure 1 based on [5 , p.13]):

- **Data sets:** identification of data sets which are available for first responders and police authorities as well as barriers to utilising these data sets (including both access as well as exchange issues in human to human, human to machine and machine to machine communication).
- **Information management processes:** identification and mapping of common work flows, decision trees, general crisis management models and lessons learnt within each European country, in order to point out the possible gaps in data sets, missing interoperability within and between organisations and procedural differences.



- **Information systems:** identification of information and communication systems, available and used by first responders and police authorities, including relevant functionalities as well as analysis of success factors and barriers for the application of information systems.
- **Business models:** analysis of business models to facilitate the cooperation between stakeholders (including Public-Private Partnerships) and application of ICT solutions into practice. In addition to considering fit between problems and solutions, also included are analyses of the fit between these business models and regional, national, European, and international regulations as well as public procurement procedures.

Purpose of this document

This document presents the final state of the inventory with regard to the aforementioned categories. While actual results are collected and maintained in a database to sustain inventory results (see integration of inventory content into the SecInCoRe demonstrator in [9] and [18] and [19] and chapter 6 “Access to inventory content”), this document summarises results in terms of

- activities and implications on the research roadmap for WP3
- structures and schemes to document inventory content
- exemplary content for all inventory categories
- implemented services to access the inventory content

While the purpose of the entire inventory is to a) gather knowledge and b) simplify access to that knowledge, the main purpose of this deliverable is to document how the SecInCoRe team gathers and structures inventory content to make it accessible by using a semantic search framework.

Validity of this document

The deliverable describes all activities carried out to create the inventory with regard to all four categories. As stated before, the deliverable does not include the complete inventory content. Further content is stored in the respective databases of the Knowledge Base.

Relation to other documents

This document has relationships with other documents created within the SecInCoRe project. The following documents are referred to in terms of foreground literature:

- [1] Grant Agreement
- [2] Consortium Agreement
- [3] Description of Work (DOW)



- [4] D2.1 Overview of disaster events
- [5] D3.1 Inventory Framework
- [6] D3.2 First Inventory Results
- [7] D3.3 Second publication of inventory results

As other WPs are connected with respective results, the following documents are also connected to D3.4:

- [8] D2.5 [in the form of T3.1 input to T2.2]
- [9] D4.1 [in the form of T3.1/T3.2/T3.3 input to T4.2]
- [10] D4.2 [in the form of T3.2/T3.3 input to T4.3]
- [11] D4.3 [in the form of T3.1/T3.2/T3.3/T3.5 input to T4.1]
- [12] D4.4 [in the form of T3.1/T3.2/T3.3/T3.5 input to T4.1]
- [13] D6.1 [in the form of T3.4 input to T6.3]
- [14] D6.3 [in the form of T3.4 input to T6.3]

As results of activities in other WPs are included in WP3, this deliverable is based on tasks which led to the following deliverables:

- [15] D1.4 [as AB activities are regarded in all Tasks of WP3]
- [16] D2.1 [in the form of T2.1/T2.3 input to T3.1/T3.2/T3.4]
- [17] D2.2 [in the form of T2.1/T2.3 input to T3.1/T3.2/T3.4]
- [18] D5.1 [in correlation to demonstrator setup in WP5]
- [19] D5.2 [in correlation to demonstrator setup in WP5]
- [20] D2.4 [in the form of T2.1/T2.3 input to T3.1/T3.2/T3.4]

All activities in WP3 are based on strong interdisciplinary collaboration with WP2 and stakeholder interaction which includes ethical, legal, and societal issues (ELSI). Thus, the research is in-line with the overall SecInCoRe approach towards those aspects and builds on

- [21] D1.2 Research Ethics

Contribution of this document

This deliverable should facilitate reflection on the research methodology (as defined in [5]) and the final inventory results. Thus it comprises a description of how inventory categories are understood and which background knowledge consortium members can bring to each category. This enables further and more detailed discussions of possible content. It helps to define validation and evaluation plans to assess the progress made in collecting items in the several tasks of WP3 and the potential benefits for all types of stakeholders (cp. [3]).

Target audience

The deliverable is a working document to facilitate collaboration within the SecInCoRe team. It was declared to be public

- to allow sharing with ‘third parties’ from related fields of research or practice (e.g., first responder, information system provider and researcher)
- to gather feedback from such experts.

As the categories of the inventory are very different, some parts of this document address specific reader groups directly while they may be hard to understand for other groups. All chapters include information to allow all stakeholder to engage with the SecInCoRe research results regarding the inventory on a general level. But if the reader wants to go into more depth, the description of SecInCoRe objectives in [3] and the FP7 Security programme (especially topic ‘SEC-2012.5.1-1 Analysis and identification of security systems and data sets used by first responders and police authorities’) will help, and there are a range of academic and media publications available at the project website <http://www.secincore.eu> that elaborate on specific aspects.

Glossary

Abbreviation	Expression	Explanation
Apache	Apache HTTP Server	The Apache HTTP Server is the world's most used web server software.
API	Application programming interface	A suet of subroutines and definitions to develop software.
BAMF	federal office for migration and refugees of Germany	BAMFs working areas are manifold, including research and many other activities in the field of asylum, migration, integration and support to the return
BM.I	Federal Ministry of Internal in Austria	The BM.I is in charge of security issues in Austria comprising citizenship, elections and national referendums.
BMJV	Federal Ministry of Justice and Consumer Protection of Germany	The directorate is responsible for the courts constitutions i.e. for Federal law regulations on the structure and organisation of the courts and public prosecution offices. The Directorate General's sphere of responsibility also includes the procedural rules for ordinary



Abbreviation	Expression	Explanation
		jurisdiction (i.e. the civil and criminal courts, including criminal investigation proceedings) as well as for administrative and financial jurisdiction.
CAP	Common Alerting Protocol	Data exchange model
CBRN	Chemical, Biological, Radiological, and Nuclear	CBRN describes the type of the hazard for the population.
CEIS	cloud-based emergency information system	Emergency information system which can be accessed via internet.
Chemdata		Chemdata is an interactive database of chemical hazards.
CSF	Critical Success Factor	CSF are limited characteristics that have direct impact on an organisation or project, because they affect their effectiveness and efficiency.
DoW	Description of Work	
DRK	Red Cross Germany	
EASO	European Asylum Support Office	https://easo.europa.eu/
EFFIS	European Forest Fire Information System	EFFIS consists of a scientific and technical infrastructure at the Joint Research Centre (JRC) doing research on forest fires and operating a web based platform and database.
ELSI	Ethical, legal and social issues	Ethical and social challenges and opportunities that arise in emergency situations, especially with a view to the use of ICT. Legal issues arising, particularly around data protection, liability, and responder safety



Abbreviation	Expression	Explanation
EMC	Emergency Management Cycle	The EMC illustrates the ongoing process of prevention, preparedness, response and recovery for disasters.
EM-DAT	Emergency Event Database	EM-DAT presents an international disaster database with essential core data from 1900 to the present.
FR	First responders	
FRONTEX		European agency - http://frontex.europa.eu/
GIS	Geographic information system	A geographic information system (GIS) is a system designed to capture, store, manipulate, analyse, manage, and present all types of spatial or geographical data.
GUI	Graphical User Interface	
HLR	High-level Requirements	HLR are the most generalised division of requirements of a system.
ICT	Information and communication technology	ICT stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software , middleware , storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.
INPOL		INPOL is a integrated information system of the German police authorities.
IS	Information systems	A computer Information System (IS) is a system composed of people and computers that processes or interprets information.



Abbreviation	Expression	Explanation
JRC	Joint Research Centre	The European Commission's in-house science service
KB	Knowledge base	A knowledge base (KB) is a technology used to store complex structured and unstructured information used by a computer system. In the SecInCoRe context the knowledge Base is the technical representation of the inventory
KPA	Key Performance Area	KPAs evaluate, measure the success of an organisation
KPI	Key Performance Indicator	KPIs evaluate, measure the success of an organisation
LDAP	Lightweight Directory Access Protocol	LDAP is a standard lightweight application protocol to manage distributed directory information.
LOD	Linked (Open) Data	Web of Data, which can be understood as one realisation of the Semantic Web
ManifoldCF	Apache ManifoldCF project	Apache ManifoldCF is an effort to provide an open source framework for connecting source content repositories
OSF	Open Semantic Framework	One core application of the Semantic Framework. Used to store data and metadata.
RDF	Resource Description Framework	A recommendation for semantic web data models
SF	Success Factors	Success factors (SF) are the “combination of important facts that is required in order to accomplish one or more desirable business goals”. [www5] Further Critical success factors (CSF) were introduced as an extension of the before mentioned SF. “Limited number (usually between 3 to 8) of characteristics,



Abbreviation	Expression	Explanation
		conditions, or variables that have a direct and serious impact on the effectiveness, efficiency, and viability of an organisation, program, or project. Activities associated with CSF must be performed at the highest possible level of excellence to achieve the intended overall objectives.” [www6]
SFTP	Secure File Transfer Protocol	N etwork protocol that provides file access, file transfer, and file management over any reliable data stream
SMART	Specific, Measurable, Achievable, Relevant and Time-bound	Guidance for the development of metrics for technology performance
SOAP	Simple Object Access Protocol	
TextSTAT	Textstatprogram	Simple programme for the analysis of texts
UN	United Nations	http://www.un.org/en/index.html
	Category entry	Entries in the inventory spanning the aspects data sets, information management processes, information systems, business models and cross-cutting ethical, legal and social issues
	Data types	Types based on descriptions of the data on a semantic level (e.g., spatial data in terms of vehicular movements)
	Stakeholder	Everyone who is involved in overcoming a disaster event



List of figures

Figure 1: Inventory content.....	10
Figure 2: Activities for the inventory of data sets	21
Figure 3: Overview countries.....	22
Figure 4: Categories of datasets	23
Figure 5: Incident types	24
Figure 6: Classification of data sets related to Disaster Management (out of [Data00] [GuBe02][HCLL10][Iasc10][MBKB15][TsBG06] [XuZI07][ZSTL10]).....	26
Figure 7: Database structure of data sets	28
Figure 8: Past disaster database scheme	29
Figure 9: Research approach for the analysis of command systems and information management (as defined and as maintained in practice) Source: Based on [5 , p. 30]	30
Figure 10: Structure of the EU and Germany related to civil protection.....	32
Figure 11: Stages of GRIP [www7]	37
Figure 12: Refugee reception centre process	39
Figure 13: Event planning process – incident situation at a stadium [BFV13] [DFB09] [FIFA16].....	42
Figure 14: Current status of activities in task T3.3.....	44
Figure 15: Database scheme for information systems (see D3.3)	46
Figure 16: Number of systems gathered in each category	47
Figure 17: Spreading of gathered information systems in the SecInCoRe Knowledge Base	48
Figure 18 Database implementation	49
Figure 19: Basic success factors by [Dorn94] and [MBP04].....	51
Figure 20: Overlapping of success factors targeting provider and users	51
Figure 21: Influence of experienced project managers on IS users SF	52
Figure 22: Influence of involved end-users on IS users SF	53
Figure 23: Influence of stable main requirements on IS users SF	54
Figure 24: Influence of a motivated and competent team on IS users SF	55
Figure 25: Research approach for the analysis of business models.....	59
Figure 26: Knowledge Base on Business Models	63
Figure 27 Structure of the business models database.....	63
Figure 28: Report on the included Business Models in the Knowledge Base.....	64
Figure 29: Report on the main for Business Models identified.....	65
Figure 30: Top Level concept of the Semantic Framework.....	69
Figure 31: Organisational concept	70
Figure 32: Standard Upload	71
Figure 33: Example of the analysis to understand relevance and content of a document	73
Figure 34: Quality assurance process	74
Figure 35: Search GUI mock-up.....	75
Figure 36: Investigation of semantic systems	76
Figure 37: Architecture diagram showing the different core components	77
Figure 38: Overview of the crawling and searching process.....	79
Figure 39: Record of one database entry.....	80
Figure 40: Search results and link to document	81
Figure 41: Overview of the SecInCoRe common GUI	82
Figure 42: Summary and topic edit mode for document search results.....	83
Figure 43: Search and Filter GUI with search results and details for sample query ‘hazard’. The Filter in the left pane allows to refine the ontology elements for filtering.....	84
Figure 44: Task dependencies [Figure part of the DOW].....	86
Figure 45: Relationship between Hypernyms and Hyponyms	87
Figure 46: Approach for the Reference Command System by definition.....	88
Figure 47: Approach for the Expansion of the Reference Command System	89
Figure 48 Generic communication architecture incl. RescueRoam (see D4.3, D4.4 for details).....	90
Figure 49: Connections between HLR and the different components	91



Structure of the deliverable

The document begins with a general part in chapter 1. The following structure of this deliverable is in accordance with the inventory artefacts regarding this work package:

Chapter 2	Final version of data sets
Chapter 3	Command systems and information management processes
Chapter 4	Research and inspection of information and communication systems
Chapter 5	Business models for to the application of information systems
Chapter 6	Access to inventory content
Chapter 7	Connection between Work packages
Chapter 8	Verification and Validation of Inventory, Knowledge Base and Search

All these chapters are divided into two major parts: The first part describes all activities undertaken, delineates compliance with and deviations from the research programme defined in [5] and illustrates the coherences between and motivations for them. The second part comprises respective results of these activities.



2 Final version of data sets

This chapter provides information about the conducted process of gathering and structuring data sets, including the description and definition of fundamental terms. It documents the origin of data sets, including respective countries, categorisation of the collected data sets, and considered incident types.

In literature, the terms 'data' and 'data sets' are often used, but there is no clear delimitation between them; sometimes they are used interchangeably. In SecInCoRe the terms 'data set' and 'database' are basic components of what?. Before the previously published deliverables focusing on the SecInCoRe inventory can be expanded, these terms need clarification. The ISO 2382 defines data as "a representation of facts, concepts, or instructions in a formalised manner, suitable for communication, interpretation, or processing by humans or by automatic means" [Inter99] [www11]. Data sets are collections of related data [www9] [www11] [www12]. One frequently used categorisation upon which to build data sets is the availability and the need for that piece of data in the information management process in an emergency or disaster [6] [7].

There are databases which collect relevant data sets related to a dedicated topic about disasters, such as health or hazard (see for example EM DAT [www10]). Other relevant databases are presented in previous deliverables of SecInCoRe especially in [8] and also [7] and are included in our own gathering approach and can be seen at secincore.eu/search.

The following subchapter deals with the collected datasets and relevant incident types. First the research approach is presented and the work done in WP3.

2.1 Approach

According to the research framework of [5], several activities have been conducted to gather information about data sets (see Figure 2).

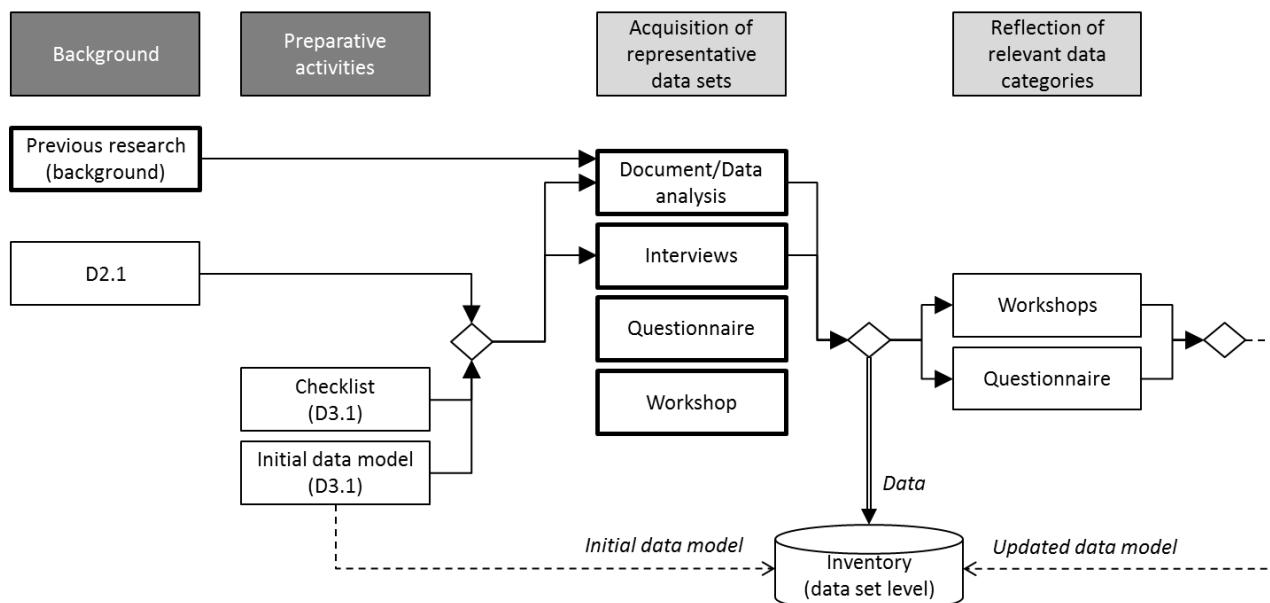


Figure 2: Activities for the inventory of data sets

- The first activity was the collection and analysis of results from **previous research** and **document / data analysis**: SecInCoRe aimed to broadly approach data gathering (i.e. linked open data, existing databases, etc.). Through an analysis of the case studies and previous disaster events, a process of identification of the fundamental building blocks for the datasets was carried out, forming a framework for structuring and utilising the information in the way that make the data meaningful and providing access to the pool of useful documentation and conclusions. This procedure has led to the formation of the templates that are made available upon usage of the SecInCoRe inventory.
- **Questionnaires** were administered based on the questionnaire created by EPISECC to use and strengthen the collaboration between the two projects and to contribute to the overall inventory approach of the EPISECC project. From SecInCoRe's side, 10 people were asked to participate in the questionnaire, all active officers: 2 from the special unit of Disaster Recovery of the Fire Corps, 1 from the Administrative Division of the Fire Corps, 1 from the Civil Protection Agency, 2 from the special unit of Antiterrorist Division of the Hellenic Police, 1 from the General division of the Hellenic Police, 1 from the Hellenic Police Intelligence Division and 2 from the Lancashire Resilience Forum. These results were combined with those from EPISECC for both projects to analyse.
- **Workshops**, based on collaborative design, were run (for example in Lancaster May 2016 and October 2016) and based on demonstration cases (for example in Paderborn October 2016) from which further data and reflections upon SecInCoRe's approach to the inventory were gathered.

2.2 Evolution of the data model

SecInCoRe researched and collected an extensive list of data sets which refer to disaster and crisis management.

The focus of gathering was on data sets that fulfil the following criteria:

- Origin of the data set
- Inclusion or contradiction to the current data model
- Incident type

Each of these criteria are explained below.

2.2.1 Origin of the data set

At first, it is important to collect data sets which affect the regions where SecInCoRe is active. This means that primary data sets with focus on European countries were gathered. Figure 3 shows the distribution of gathered data sets to the various countries. The focus is on data sets which give Pan-European or worldwide information. Further data sets with relevance to the topic were included in the inventory.

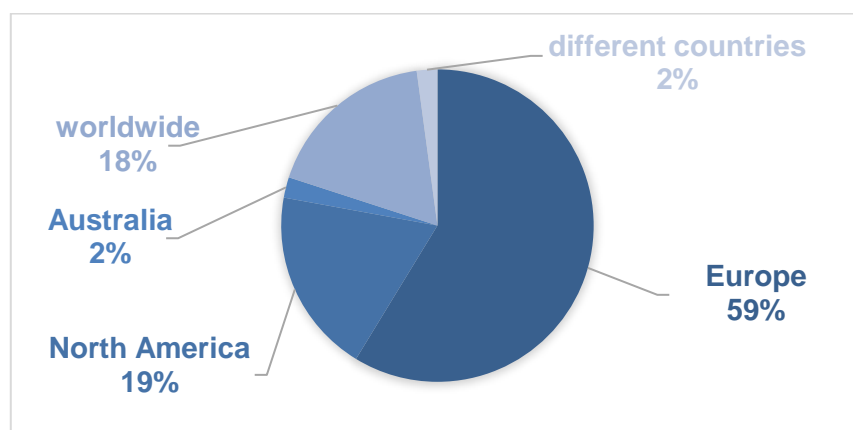


Figure 3: Overview countries

2.2.2 Inclusion or contradiction to the current data model

Data sets were gathered based on the emergency management cycle. Within the four phases, a further subdivision was useful to structure the gathered data. Figure 4 shows the different categories of gathered data sets and the first basis of the data model.

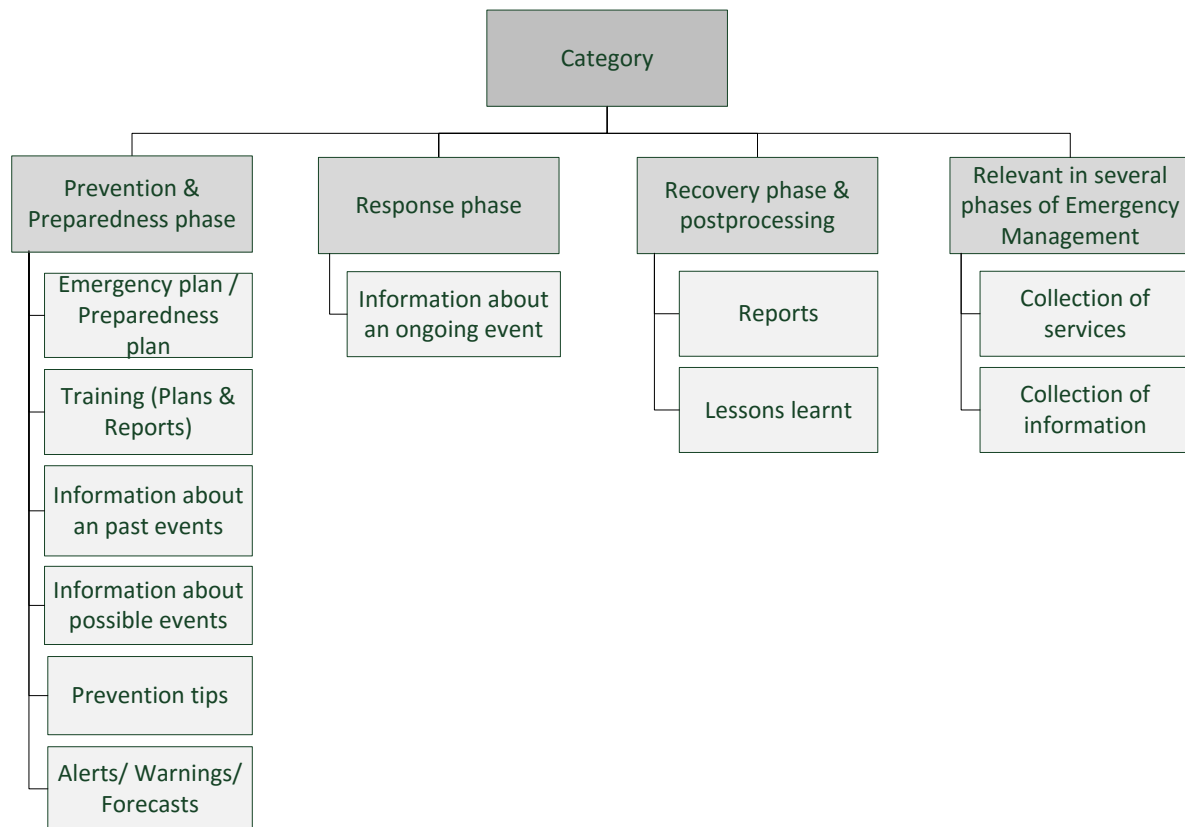


Figure 4: Categories of datasets

In the different phases of an emergency (Emergency Management Cycle (EMC)) [Bair10] [Warf], organisations need various information. Therefore, different types of data sets were gathered to cover different needs of information. SecInCoRe's focus is on the **prevention and preparedness phase**. It is necessary to have information about how to react in case of an emergency (emergency plans or preparedness plans) as well as suggestions on how to train for different scenarios. Additionally, it is important to have information about possible future events as well as information about events that occurred in the past. It is also important to include data sets which give forecasts and warnings of impending events.

During the **response phase** it is important to stay up to date about the event. Therefore, data sets are gathered which also give information about already ongoing events. So organisations may get real time information and react more quickly.

During the **recovery phase and post-processing** it is necessary to analyse decisions and processes and to adjust the emergency management system. So in this phase organisations need documentation, reports and analyses about past events.

Moreover, there are data sets that are **relevant in several phases** of emergency management like collection of services or information which may be needed in different phases.

2.2.3 Incident type

During the gathering of data sets a distinction between different incident types were made. Most data sets are relevant for just one specific incident type. So data sets were gathered that covered as many incident types as possible. Figure 5 **Fehler! Verweisquelle konnte nicht gefunden werden.** shows which incident types were considered (based on [PBBT+14, p. 25] and [4]).

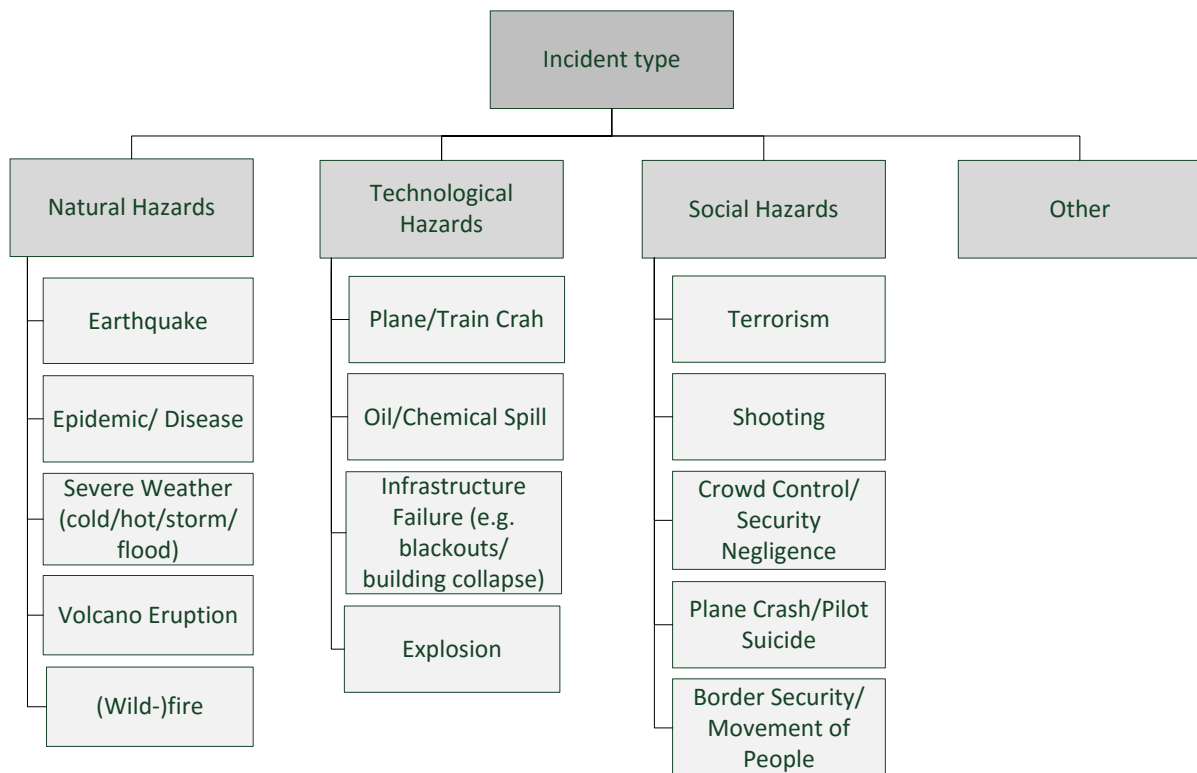


Figure 5: Incident types

2.2.4 Reflection of the data model

The first categorisation of data sets with the EMC (Figure 4) contains some weak points. Primarily the EMC as a tool for the categorisation is difficult, because sometimes it is not possible to differentiate one phase from the following one. The delimitation depends on different aspects, for example the duration of an incident and the incident type.

Furthermore, there are data sets which are not assigned to only one EMC phase, because this information is available during the whole cycle like a collection of services. Other information sets are assigned to one phase, but exactly these information are necessary for another phase to process and create new guidelines for the preparation of possible, future incidents. Because of these problems with these categories and assigning data sets to single categories, we started another literature research and remarks of Co-Design or Advisory Board workshops to rework the division.

This includes:

- Literature
- Internet search
- Review of workshop results
- Reflection of other research projects

The revision of existing classification of data sets related to disaster management designed was far from straightforward. The first challenge constitutes the choice of the search criteria, because there are a lot of synonyms for the same or similar terms or the same terms meaning different things. For the search, we used, for example, the search criteria 'categories of datasets for crisis management'. After there were less good results to support coming to a conclusion of a categoration scheme, a change of the search term and way searching was necessary. So 'disaster management' replaced 'crisis management'. The absorption of relevant documents after using similar terms was better than before and the results contain some new documents, which were not listed before. The literature research comprised many additional search terms and literature results. The description above should illustrate the necessity of different word combinations and the use of synonyms. Another challenge constitutes the documents itself. Several documents possess a title, keywords or summary that does not reflect the content of the whole document. Despite all challenges, the research creates some usable results. In the following paragraphs, the findings and the implementation in relation to the first categorisation (Figure 4) of data sets will be described.

2.2.5 Final data model

At first there is no standardised definition, methodology and categorisation of data and data sets [GuBe02]. Researchers use different data sets to create a new model or methodology in several areas. Only a few scientists try to create a rough classification of necessary data sets in relation to disaster management. There is a notable frequency of the category 'operational' data sets [BAZZ09][Huma00][HaHa14][Iasc10][XuZi07] with a few more data sets listed. Other categorisations of data sets are based on data exchange formats and are limited to that purpose. To create a useful categorisation for SecInCoRe we collected all data sets listed in several papers, books and sources. Some data sets, like geographic data, were detected multiple times. Following we assigned the data sets to useful categories. The method of "Clustering" is a process of organising objects into groups whose members are similar in some way. [Alde84] It can be scored by several algorithms that vary in their notion of what constitutes a cluster and how to efficiently find them. The aim of clustering is to determine the intrinsic grouping in a set of abstract data. (Xu09) In case of SecInCoRe the clustering was conducted in a manual way. The categorisation occurs in consideration of the detected general data set names. The establishment of the first level with the two types of distinction is a combination of the research papers related to data sets and also a paper with a division of databases. [TsBG06] includes a clear differentiation between the area (e.g. national, regional,...) and the disaster-dependent databases. The allocation of each single data set to a top level class builds up the arrangement at Figure 4, the EMC phases, but the classification is made by the speed of changing of the single information. Therefore, the categorisation of data sets that changes very slow or not at all, data sets that changes every time after an incident occurs and datasets that changes multiple times during a disaster were used. The summary of the results is shown in Figure 6.

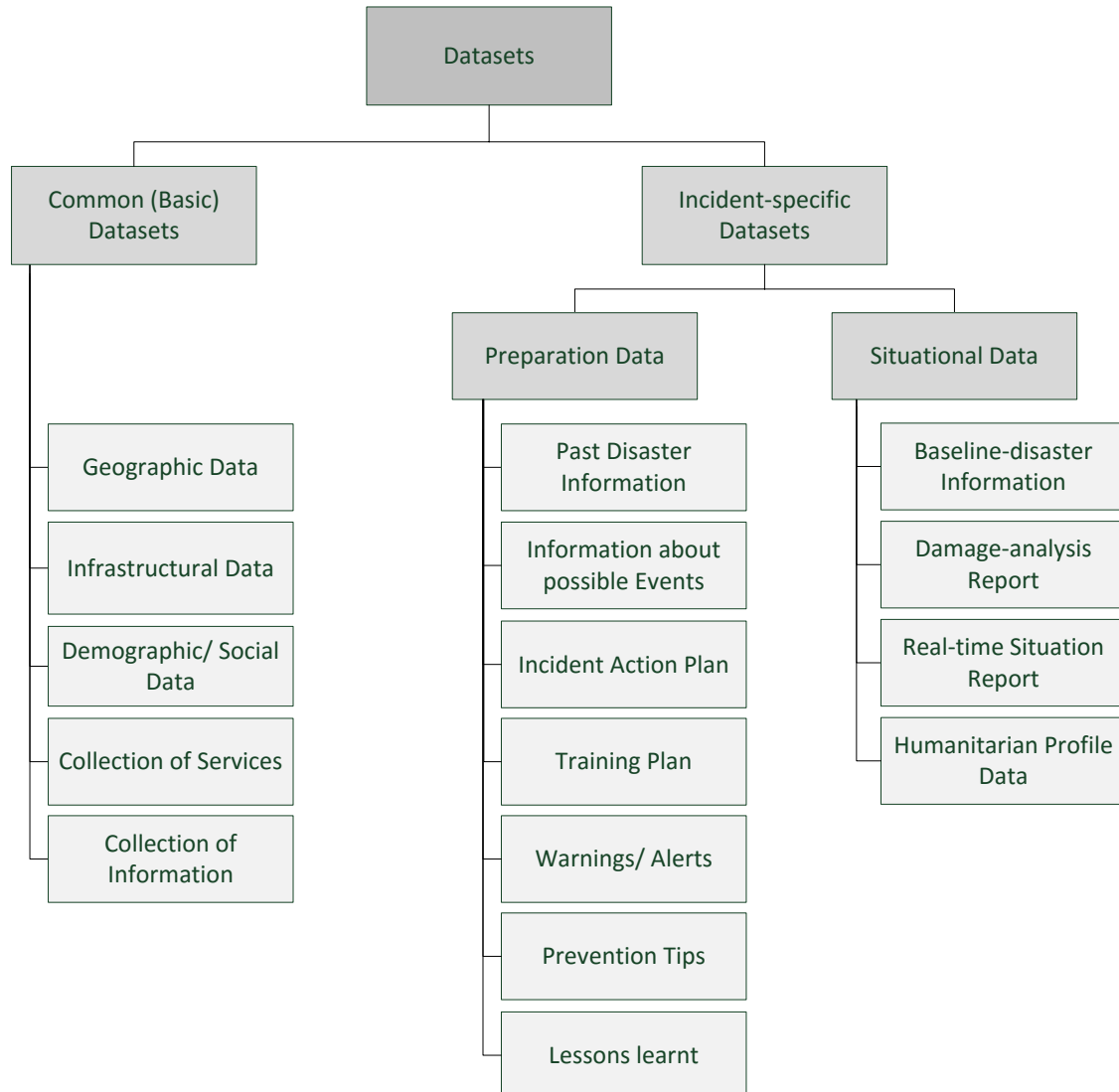


Figure 6: Classification of data sets related to Disaster Management (out of [Data00] [GuBe02][HCLL 10][Iasc10][MBKB15][TsBG06] [XuZI07][ZSTL 10])

The figure above shows that we divide data sets into two main categories, the common (basic) datasets and the incident-specific data sets.

Common (basic) data sets are almost static data. The information will be collected once and modifications will be relatively rare. This category includes geographic, infrastructural, logistical, demographic, and social data. Furthermore, a collection of services and information like organisations that belong to the disaster management teams (e.g. the fire department, emergency service and the police) and all necessary information about them (e.g. telephone numbers and organisational practices in case of an incident for the general public) are contained in this main class.

The second main category, incident-specific, is more dynamic in contrast to the common data sets. Since the single data sets of this class changes with different speeds, it is necessary to develop sub-categories. The first one, the preparation data, changes very

slowly. Therefore, an incident action plan and information about past and possible events amongst others belongs into this area. For example, the action plan has to be re-worked after a new disaster occurs, because there is new information and situational circumstances that should be considered for the next incident. Data sets inside the second subcategory, situational data, change fractionally very quickly. This includes baseline-disaster information and humanitarian profile data and some additional data sets. Humanitarian profile datasets comprise e.g. information about the amount of affected and injured persons after a disaster occurs. This kind of information changes during the response and recovery phase. After an incident occurs there are initial valuations, but as time goes on the information about injured or dead persons will be updated again and again.

On the basis of the data set categorisation, shown at Figure 6, furthermore the level of usefulness can be assigned to the single data sets. [PBBT14] pointed out that there are three levels of usefulness. Data set “can be useful because they are commonly used and have been proofed and tested” [PBBT14, p. 205]. Other data sets are untested, but they “can be useful because it is the only one that can be used to provide a particular set of knowledge” [PBBT14, p.205]. The last level contains data sets which do not really exist, “but are pointed to as having been useful by the lessons learned or problems faced during a disaster” [PBBT14, p.205]. This kind of categorisation can be applied on Figure 6. Certainly this new classification is a valuable combination of the before mentioned categories of data sets:

- available and used
- available and shared
- available and not used
- not available but needed
- not available in some organisations but available in others

The categorisation of data sets, shown at Figure 6, corresponds with the identified incident types for SecInCoRe. The relevant data sets related to disaster management depend on the incident type. Figure 6 illustrates the relationship amongst others through the headline incident-specific datasets.

2.3 Publication of Data Sets

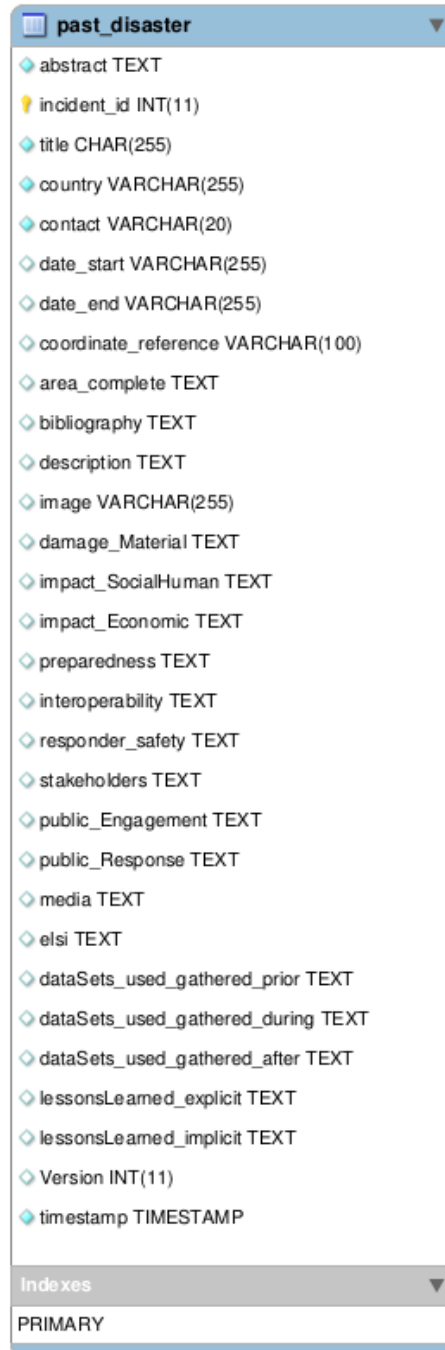
Data sets as part of the inventory are stored in a dedicated database of the Knowledge Base. The structure is shown in the Figure below.



Datasets
ID INT(11)
◇ Title TEXT
◇ Comment TEXT
◇ Link TEXT
◇ Language TEXT
◇ Country TEXT
◇ Publisher TEXT
◇ Prevention/Preparedness_Phase TINYINT(1)
◇ Emergency_Plan/Preparedness_Plan TINYINT(1)
◇ Training_(Plans/Reports) TINYINT(1)
◇ Information_about_past_events TINYINT(1)
◇ Information_about_possible_events TINYINT(1)
◇ Prevention_tips TINYINT(1)
◇ Alerts/Warnings/Forecasts TINYINT(1)
◇ Response_Phase TINYINT(1)
◇ Information_about_an_ongoing_event TINYINT(1)
◇ Recovery_Phase/Postprocessing TINYINT(1)
◇ Reports TINYINT(1)
◇ Lessons_Learned TINYINT(1)
◇ Relevant_in_several_phases/Other TINYINT(1)
◇ Collection_of_services TINYINT(1)
◇ Collection_of_information TINYINT(1)
◇ Natural_Hazards TINYINT(1)
◇ Earthquake TINYINT(1)
◇ Epidemic/Disease TINYINT(1)
◇ Severe_Weather_(cold/hot/storm/flood) TINYINT(1)
◇ Volcano_Eruption TINYINT(1)
◇ (Wild-)fire TINYINT(1)
◇ Technological_Hazards TINYINT(1)
◇ Plane/Train_Crash TINYINT(1)
12 more...
Indexes
PRIMARY

Figure 7: Database structure of data sets

Further as one part of the SecInCoRe data model the scheme of the past disaster database is presented. The database structure goes beyond the categorisation of incident types. A detailed description is provided in [8] and also demonstrate the connections between the different database elements.



past_disaster	
abstract	TEXT
incident_id	INT(11)
title	CHAR(255)
country	VARCHAR(255)
contact	VARCHAR(20)
date_start	VARCHAR(255)
date_end	VARCHAR(255)
coordinate_reference	VARCHAR(100)
area_complete	TEXT
bibliography	TEXT
description	TEXT
image	VARCHAR(255)
damage_Material	TEXT
impact_SocialHuman	TEXT
impact_Economic	TEXT
preparedness	TEXT
interoperability	TEXT
responder_safety	TEXT
stakeholders	TEXT
public_Engagement	TEXT
public_Response	TEXT
media	TEXT
elsi	TEXT
dataSets_used_gathered_prior	TEXT
dataSets_used_gathered_during	TEXT
dataSets_used_gathered_after	TEXT
lessonsLearned_explicit	TEXT
lessonsLearned_implicit	TEXT
Version	INT(11)
timestamp	TIMESTAMP

Indexes
PRIMARY

Figure 8: Past disaster database scheme

3 Command systems and information management processes

This chapter aims to provide an overview of command systems and also information management processes. The first sub-chapter includes EU institutions and the organisations of their member states related to disaster management. Thereby the first step presents a literature review. On the basis of this review, an overview of the institution, information systems and the possible connection between them was created. Following there is a selection and description of the relevant command and control systems. At least there are two examples of information management and command and control systems in practice. The first one contains a refugee reception centre process and the second one presents an event planning process (i.e. planning of an incident in relation to a soccer game) .

Before starting with the sub-chapters, the term ‘process’ has to be clear. Generally a process is a series of coherent activities. It works only with input and results in one or more outputs [Füer14]. A process can be found in every area, e.g. production, business or computer science [www13].

The remaining part of this chapter contains an analysis of command systems and of information management processes.

3.1 Approach

According to the research framework of D3.1, several activities have been conducted to analyse the command systems and information management processes of first responder and Police Authorities. In the following is the extended figure of the research approach:

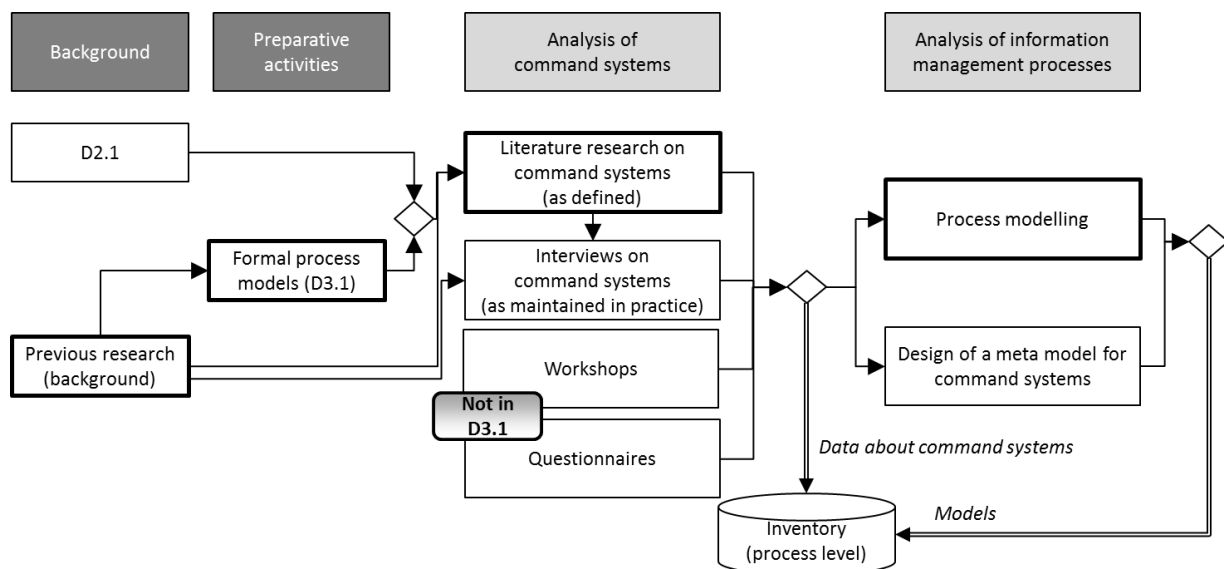


Figure 9: Research approach for the analysis of command systems and information management (as defined and as maintained in practice)

Source: Based on [5 , p. 30]



- Literature research on high-level processes and existing command systems (based on the ISO 22320, DV-100, SCMW, GRIP and the ICS deviations between the command systems were analysed and illustrated).
- Process modelling: especially ISO 22320 was in focus to extract relevant tasks and relevant information
- Defining relationships between used processes and the occurrence of data sets and used information systems

3.2 High-level perspective of information management process related to emergency management

The connection between institutions of the European Union (EU) and the organisations of their member states are especially visible at major events, e.g. after natural disaster like flooding, the current refugee crisis or large CBRN incidents. The following Figure offers a general insight into these structures by the example of Germany. At this the focus is on the institutions with regard to civil protection and disaster management.

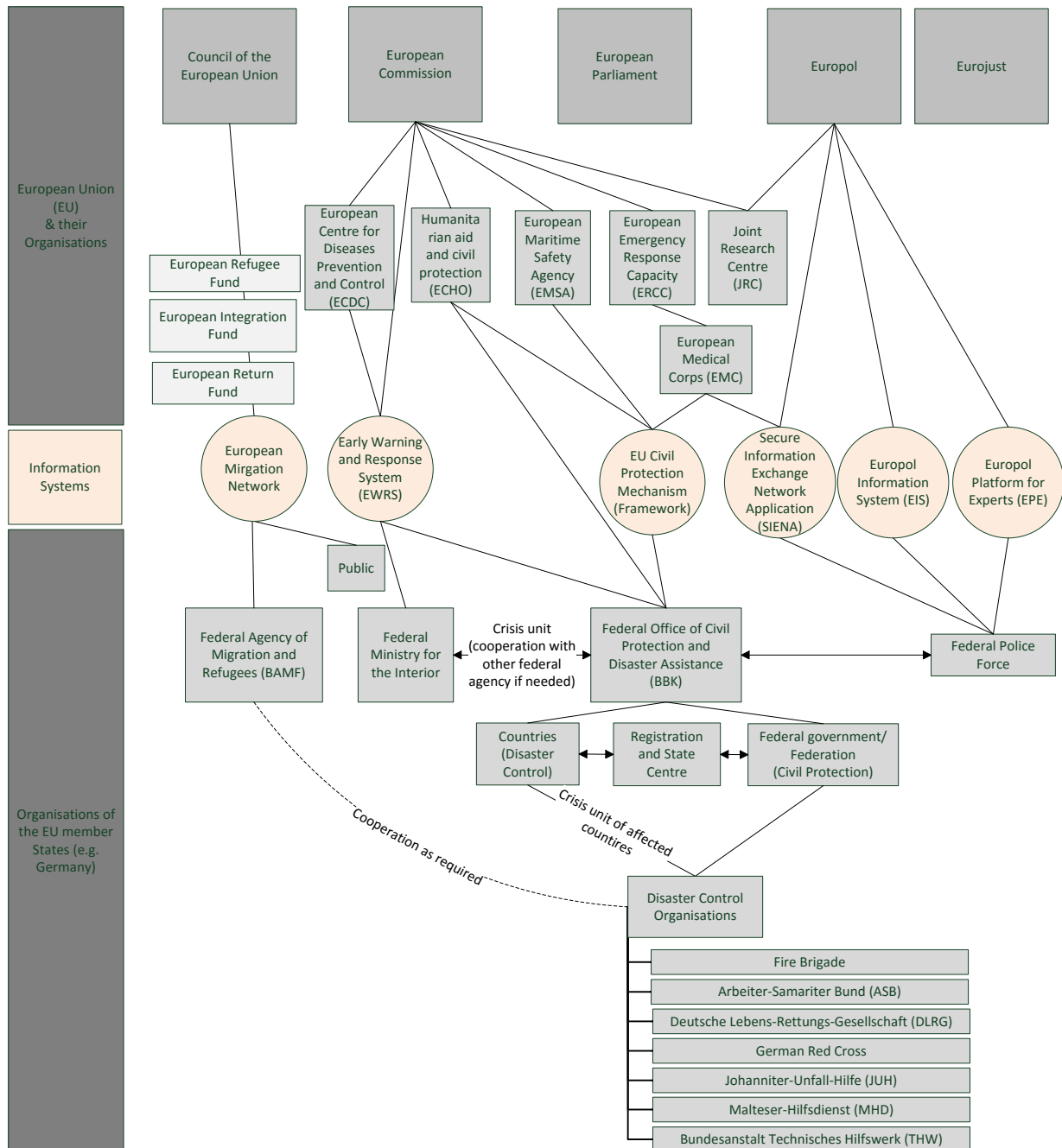


Figure 10: Structure of the EU and Germany related to civil protection

The Figure above necessarily includes a lot of different elements. In the first instance there are some EU institutions (e.g. European Commission and Europol), but the list is not definitive. These institutions are in contact with organisations of the EU like the Humanitarian aid and civil protection (ECHO). The exchange of information between the EU organisations and the organisations of the member states is made by information systems (orange bubbles in the figure above), e.g. the early warning and response system (EWRS) and also in direct discussion with representatives. For the description of the connection between the elements and an example, it is necessary to know what organisations and information systems are in the figure and what kind of tasks they have. The starting point for this deliverable are the organisations at the EU level.



The aim of the **European Centre Diseases Prevention and Control (ECDC)** is to strengthen Europe's defences against infectious diseases. To achieve this aim the ECDC offers a wide range of tasks and programs. This includes disease programmes, epidemic intelligence, health communication, preparedness and response, scientific advice, surveillance and training. [www15]

The **Humanitarian aid and civil protection (ECHO)** was built by the EU Commission as a mechanism for disaster response. ECHO deals with saving and preserving life, the prevention and alleviation of human suffering and safeguard and at least the integration and dignity of the population affected by natural disasters and man-made crisis. [www16]

The **European Maritime Safety Agency (EMSA)** “provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long range identification and tracking of vessels”. [www14]

The **European Emergency Response Capacity (ERCC)** was created for a faster and more predictable response to disasters. This organisation “provides a full 24/7 capacity to monitor and coordinate response to disasters. The ERCC collects real-time and early warning information on disasters, monitors hazards, prepares plans for the development of resources, (...), works with the participating states to map available assets and coordinates EU’s disaster response efforts.” [www17]

The **European Medical Corps (EMC)** is one section of the ERCC. [www18]

The **Joint Research Centre (JRC)** “support EU policies with independent evidence throughout the whole policy cycle. Its work has a direct impact on the lives of citizens by contributing with its research outcomes to a healthy and save environment, secure energy supplies, sustainable mobility and consumer health and safety”. [www19]

The main goal of the law enforcement agency **Europol** “is to achieve a safer Europe for the benefit of all EU citizens”. For this the agency offers special services for all member states. This includes a “support centre for law enforcement operations, hub information on criminal activities and at least a centre for law enforcement expertise”. [www20]

All affected institutions need information systems to exchange information in case of a threatening or occurring incident. In the following these systems will be described.

The **Early Warning and Response System (EWRS)** is used “in the context of communicable diseases threats. It is a web-based system linking the Commission, the public health authorities in member states responsible for measures to control communicable diseases and the ECDC. (...) EWRS is frequently used for notification of outbreaks, exchange of information and discussion about the coordination of measures among players”.

Other systems in the field of health threats are RAS BICHAT and RAS CHEM. “RAS BICHAT is a rapid alert system used for exchanging information on health threats due to deliberate release of chemical, biological and radio-nuclear agents.” The focus of RAS CHEM lies on the “exchange of information on incidents including chemical agencies relevant to terrorism and other events leading to release of chemical, and consultation and coordination of counter-measures”. [www22]



In support of the field officers the EU provide the **Civil Protection Mechanism**. This framework contains the following tools: Emergency Response Coordination Centre (ERCC), Common Emergency and Information System (CECIS), Training programme and Civil Protection modules. [www25]

The **Secure Information Exchange Network Application (SIENA)** ensures “the secure exchange of sensitive and restricted information. The platform enables the (...) exchange of operational and strategic crime-related information among Europol’s liaison officers, analysts and experts, member states and third parties with which Europol have cooperation agreements”. [www21]

Europol Information System (EIS) is another framework which is used by Europol and their member states. This system is “Europol’s central criminal information and intelligence database. It covers all of Europol’s mandated crime areas, including terrorism. The data in the EIS is stored within different online “entities” corresponding to actual objects such as cars and identity documents, and to people. The online “entities” can be linked to each other in different ways so as to create a structured picture of a criminal case. The system also allows the storage and automatic cross-checking of biometrics (DNA) and cybercrime-related data.” [www23]

Europol Platform for Experts (EPE) “offers a set of generic functions that are customised according to the needs of each online expert community. The current core functionalities include the following:

- a library, where various documents, still images and videos can be uploaded and shared within your expert community;
- a message forum, where users can ask questions and discuss issues with one another;
- a blog, where users can publish news, promote events and announce changes to their expert community;
- a calendar, where users can schedule events or meetings for a community;
- a wiki, where users can work together to build a knowledge base within their expert community.

The EPE currently hosts more than 30 platforms covering a wide range of law enforcement areas.” [www24]

The **Medical Intelligence System (MEDISYS)**” is an internet monitoring and analysis system developed by the Commission Joint Research Centre (JRC) for the Health and Consumer Protection Directorate General (DG SANCO) to identify potential threats to the public health using information from the Internet. These ‘threats’ include both communicable disease and chemical, biological and radio-nuclear threats which could have a widespread impact on the health of the European Community. “MEDISYS collects articles from various sources on Internet. Articles are classified in pre-defined categories. Statistics are stored on the filtered categories and an algorithm is used to detect ‘breaking news’ in a given category. Based on the level of new articles and the detected keywords, an alert may be sent to key persons by email or SMS.” [Euro07]



The **Common Emergency Communication and Information System (CECIS)** is “a web-based alert and notification application enabling real time exchange of information between participating states and the ERCC.” [www25]

Each country builds procedures of crisis prevention and response on defined command and control systems. In the following section, a few systems are listed.

3.2.1 Selection of Command and Control Systems

The first step is a literature review to get an overview of the following command systems.

- ISO 22320:2011 ‘Societal security – Emergency management – Requirements for incident response’
- FwDV 100
- National Incident Management System (incl. Incident Command System)
- ‘Tactics, command, leadership’ - Swedish Civil Contingencies Agency

The main focus was on the analysis of fundamental structures, processes and activities in the mentioned command systems. Afterwards the objective was to identify differences and commonalities between the command systems, which led to the development of a representative taxonomy. The comparison was done manually by selecting all relevant terms in the different command and control system and their respective definitions. This Reference Command System should represent a consistent combination of all identical or rather similar elements that are essential for a basic command system in the field of emergency services identified by their individual definitions in the command systems. Further information are provided in D3.3 and D4.3 where the approach is described in more detail.

ISO 22320:2011 ‘Societal security – Emergency management – Requirements for incident response’

The international norm ISO 22320 requirements for incident response that support private, public and governmental organisations by the execution of different incidents. The standard provides a framework for command and control, operational information and collaboration within an incident response organisation. It affects different levels, such as international, national and regional. The aim is to achieve a cross-national orientation to this norm, which supports all involved organisations and improves the efficiency of incident response operations. [ISO11, p. 1]

FwDV 100

The National unified fire service regulation (FwDV 100) applies to the fire services in all federal states of Germany, and is used as one important example within the EU. It consists of comprehensive guidelines and regulations to ensure uniformity referring to the organisational structure and relevant processes of all fire services. There are specifications for the command organisation, command process and appropriated means, that can be adapted flexibly to different kinds of incidents. The intention is to facilitate target-oriented incident response and improve the cooperation between fire



services of different federal states, as well as the collaboration with other agencies and institutions. [FwDV100, p. 2]

National Incident Management System (incl. Incident Command System)

The National Incident Management System (NIMS) describes a comprehensive and standardised approach for efficient incident management, which is applicable to all involved organisations in the USA. Therefore, different legal structures are underlying, but nevertheless NIMS is analysed for similarities in the command & control structure. The system provides a flexible framework for many different types of incidents, independent of cause, size, location or complexity. The level of validity is defined as nationwide, so that collaborative incident response is ensured. It determines processes, methods and structures for the organisations and encompasses different phases, such as prevention, protection, response, mitigation and recovery. [NIMS, p. 1ff.]

The Incident Command System (ICS) is a fundamental component of NIMS and contains a standardised management system that combines facilities, equipment, personnel, procedures and communications operating in an organisational structure. It supports the co-ordinated execution of occurring incidents. [NIMS, p. 45ff.]

'Tactics, command, leadership' - Swedish Civil Contingencies Agency

In the concept 'Tactics, command, leadership' the focus is on an efficient execution of incident response operations, including all necessary measures for the preparation of fire and rescue services. The authors describe some obvious aspects, such as tactical principles, management systems and leadership, but on the opposite also less obvious aspects. These are for example time and space and situational perceptions. In the literature both types of aspects are equally important, because of significant relationships between several aspects. The concept systematically adds the less obvious aspects to generally existing and widely recognised aspects. Furthermore the influencing factors of incident response operations are enlarged. The content deals especially with the leadership role and management staff. It provides all organisational structures and procedures for the involved organisations. [SCMW05, p. 7ff.]

GRIP

The GRIP system (Gecoördineerde Regionale Incidentbestrijdings Procedure) can't be used for the analysis. According to a statement of the IFV (Instituut Fysieke Veiligheid) there is no valid translation of the whole GRIP system available. The English translation of GRIP does not include adequate information for the development of a consistent process model. The abstract is useful to get a first impression of the underlying concept, but nevertheless it does not provide enough information for a detailed analysis.

Summary:

GRIP is an emergency management procedure, which is used by all emergency services and governmental agencies in the Netherlands. The procedure is divided into several different stages. The assignment to a specific stage depends on the dimension



of an incident and especially on the affected area. The measures for incident response can be adapted flexible to the current GRIP stage. [www7]

<u>Phase</u>	<u>Affected area</u>
GRIP 0	Source-suppression. Day-to-day routine operations, no special coordination necessary
GRIP 1	Source-suppression. Incident of limited proportions, harmonisation necessary between the various emergency services.
GRIP 2	Source-and-effect suppression. Incident with a definite effect on the surrounding area.
GRIP 3	Threatened well-being of (large groups of) the population within a single municipality.
GRIP 4	More than one municipality
GRIP 5	GRIP 4, multiple regions
GRIP State	Guidance by state required to preserve national security

Figure 11: Stages of GRIP [www7]

The selection of command systems (exclusive of GRIP) is based on an accordance of the main intentions and functionalities, because every system tries to ensure a standardised execution of incident response operations. The involved organisations and other institutions have to act according to the specified guidelines or rather requirements of the concepts, which should provide more efficiency and additionally improve the results of multi-organisational operations. Besides the mentioned command systems apply to the organisations, fire services or rescue services as an obligation in their respective countries. The commonalities are the prerequisites for the following analysis that intends to identify 'connecting-points' with regard to the content, knowing that some of these 'connecting-points' could be too abstract to be implemented. Eventually the amount of 'connecting-points' is a reference for the potential and extent of a Reference Command System, which consists of representative basic elements that are available in the above-named, already existing, command systems. In order to take country-specific differences into consideration, the selection includes several areas of validity. In addition to command systems with relevance for European countries, the National Incident Management System (incl. Incident Command System) represents a perspective outside of the EU and may reveal partial, but significant differences. There is a possibility to compare elements individually and objectively, because every command system contains necessary basic elements (see D4.3, D4.4) in their structure. Furthermore, the definitions of these elements are nearly identical or at least similar.



After visualising the single command systems in hierarchical process structures, the next step is to develop the taxonomy of a Reference Command System in relation to WP4, which provides a hierarchical structure of all identical elements.

3.2.2 Information management and command and control in practice

After this short description of the main functions and tasks of the organisations, information systems they use and existing command and control systems in Europe, now the cooperation and information flow between some of them will be given in a short example. For this the refugee crisis, with last year's peak for Germany will be used.

After the refugees arrived at their target country they were carried to the appropriate collection point by bus or train. Here the members of the disaster control organisations and the volunteer organisations care for the arriving people by supporting the registration process and offering medical care. In addition, they take care of the basic needs like food and beds. After the registration process is concluded the displaced persons are distributed to their permanent accommodation. The whole process of arriving, registration and distribution of the refugees at a refugee reception centre can be structured more in detail. All the sub-processes, as derived from the concrete events in Dortmund, September 2015 -- including the involved organisations, the information systems and the necessary data -- are shown in Figure 12..

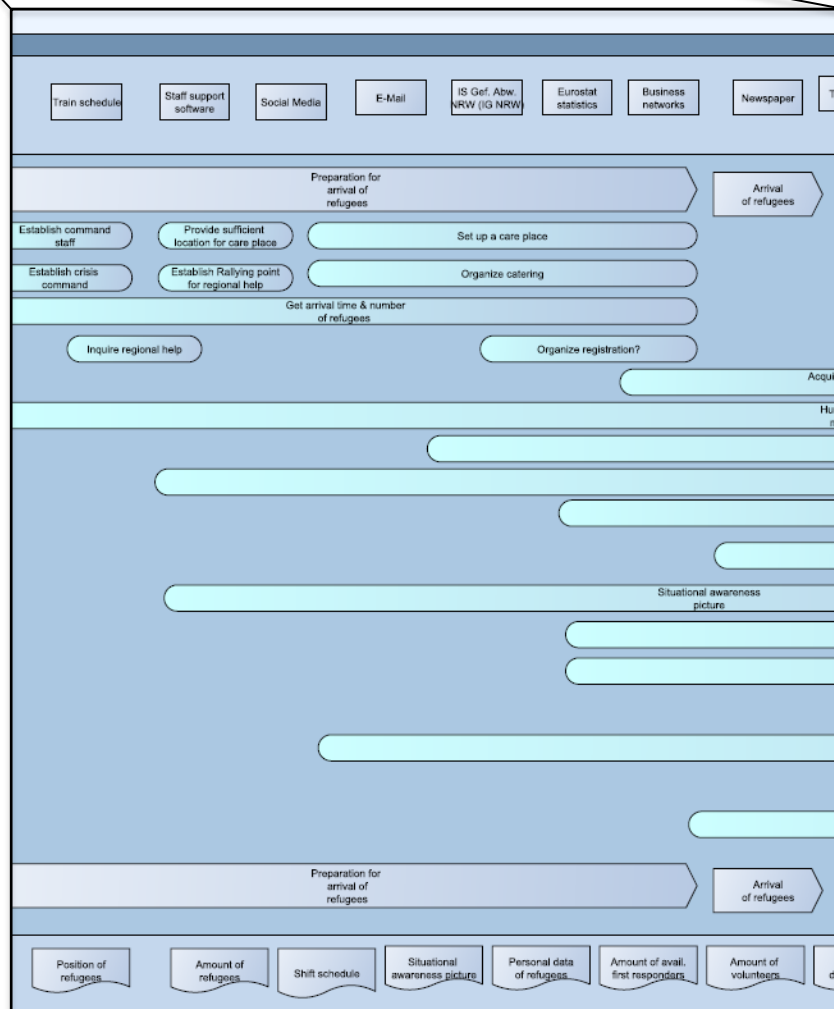
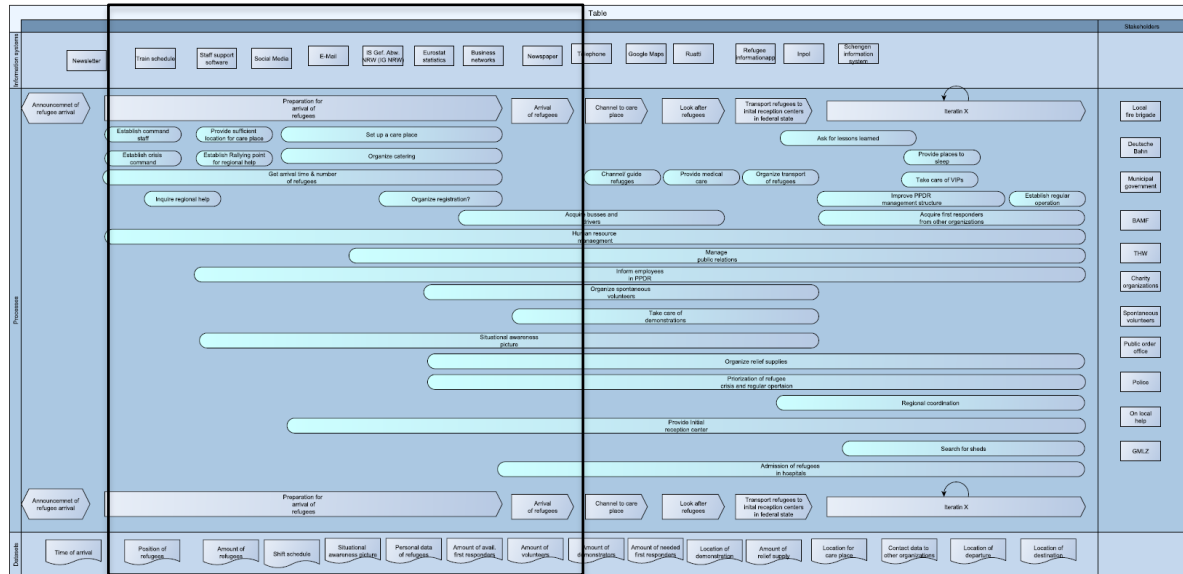


Figure 12: Refugee reception centre process



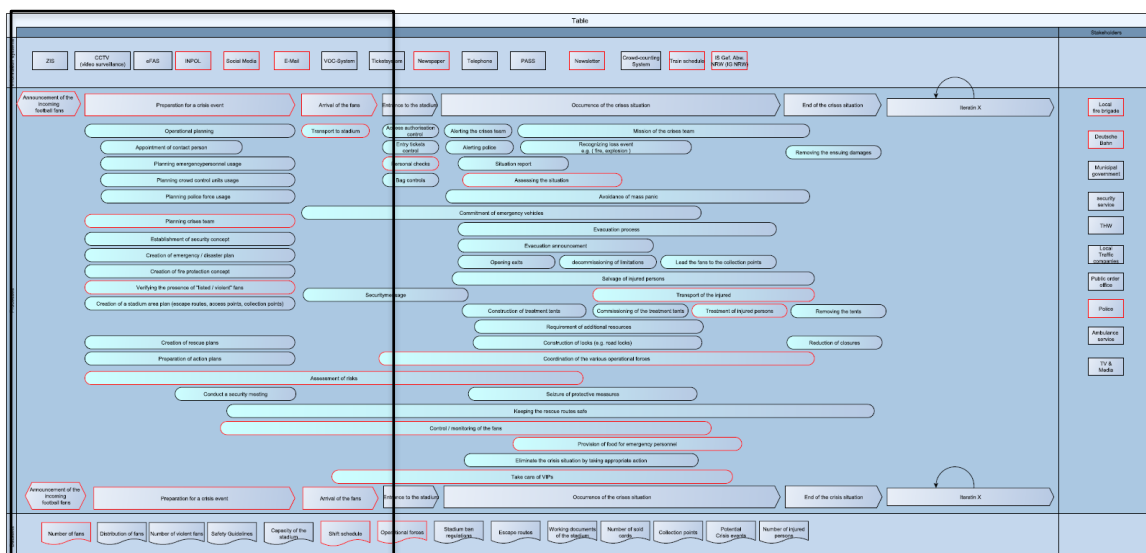
The sub-processes of the procedure on the refugee reception centre in Dortmund are assigned to the chronological main processes on the top of the process part of Figure 12. This means, that the arriving refugees in Dortmund are not in urgent danger. It starts with the main process “announcement of refugee arrival” and goes on with the preparation for the arrival of refugees, the actual arrival of them, the transport to care places, the basic medical and food care and as the last process the transport of the refugees to subsequent reception centres in the federal states. For example, the main process “Preparation for arrival of refugees” can be divided into the establishment of a command staff and crisis command, the organisation of the registration, setting up a care place and among others the request of the arrival time and the number of the arriving refugees. Many disaster control organisations, like the local fire brigade, the municipality and the Red Cross, are involved to ensure a smooth operation. But for this, they need important datasets such as the arrival time and the number of refugees to get a situational awareness picture. This was derived by various internal documents of the involved Fire Brigade in Dortmund, results from the deliverable D3.3 and interviews conducted with involved parties in the incident. To receive this information, the involved organisations use different information systems. For instance, they used social media, ‘INPOL’ and the Schengen information system for gathering the necessary information. [FwIS03][FwIS04][FwIS05][FwIS06][FwIS07][FwIS08] [FwIS09][FwIS11] [FwIS13][www1] [www2]

The general elements of the refugee reception centre process namely the main processes, the sub-processes, the stakeholder, the information systems and the necessary datasets, can be found at each process. But to compare the refugee crisis with other types of crisis or incidents, a common understanding of the connection between process, information system and data was needed. For that reason, a dedicated workshop during a meeting with experts and advisors in Lancaster took place (see D4.4). Based on the results, another process structure was conducted using a total different incident but having similarities: a fully-booked football match. Figure 10 shows this structure.

The analysis of the different incident situations shows the existence of accordance inside the processes and the involved persons, information systems and datasets. In the planning phase, there is always the preparation of the event itself and possible critical situations. For this, the organisers need certain datasets like the amount of person who are expected at the event. Based on this knowledge, the organisers are able to coordinate all relevant stakeholders. As shown in



Figure 13 the fire brigade is always one of these stakeholders but, for example, the involvement of the Police differs. Ultimately each incident situation contains identical parts. So, the organisers can look at past events and use the knowledge out of this to plan for new one.



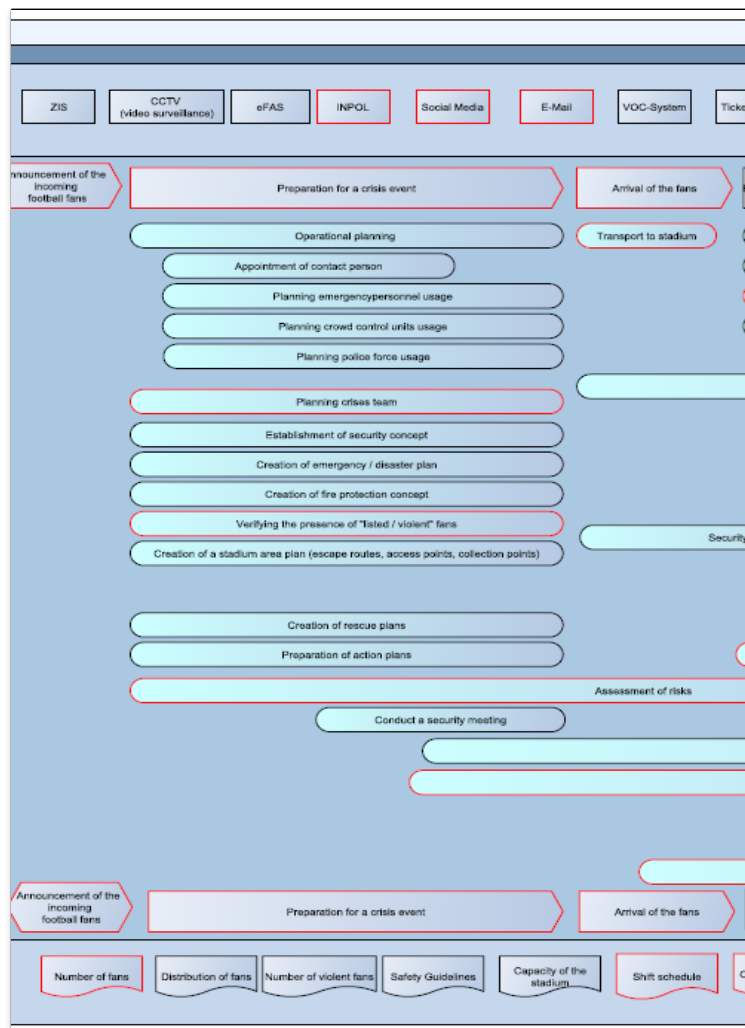


Figure 13: Event planning process – incident situation at a stadium [BFV13] [DFB09] [FIFA16]

In the run-up of such a game, there are a lot of tasks the responsible persons have to fulfil. Therefore, the main process starts with the announcement of the incoming football fans and goes further with the preparation for such an event, the arrival of the fans and the entrance into the stadium to the occurrence of a crisis situation and the end of this situation. Looking at the example below this structure can be divided into sub-processes. For this we pick up the preparation for an incident situation. This part of the structure includes among others the planning of a crisis team, the verification of listed or violent fans that may have tickets for the game and the establishment of a crisis plan. This instance is not only an example for similarities at the main process level; also, the sub-processes without the last point are identical in the description to the refugee crisis. The accordance between these two structures is not finished at this point.

In the range of the main processes some commonalities could be identified for the specific examples. The similarities are at the beginning of the whole process and start with the announcement of the incoming football fans, goes further with the preparation for a crisis event and ends with the arrival of the fans. In the subsequent process



sequence, there are no more commonalities with the refugee crisis. But if we look at the next level, the sub-processes, there will be commonalities not only in the field of the processes mentioned before, but also in the area of the main processes which are comparable with the first structure in Figure 12. For example, in the range of the entrance to the stadium there need to be person checks which are also necessary during the arriving of the refugees. Another instance can be found in the field of the occurrence of the crisis situation which is one of the most important points listed. At the beginning of a crisis situation the responsible persons have to gain an overview of the situation. Furthermore, during a crisis situation at the stadium there are additional commonalities in the other categories like stakeholder, information systems and the necessary datasets. All these commonalities of the two structures are marked with a red border in

4 Research and inspection of information and communication systems

Useful information is the key factor to enable a purposeful response to or preparation for a disaster. Information systems (IS) are valuable support targeting the provision of adequate information and therefore, a special artefact of the SecInCoRe inventory.

4.1 Approach

The approach for research in this area was defined in [5]. In accordance to this respective activities have already been conducted (see Figure 14).

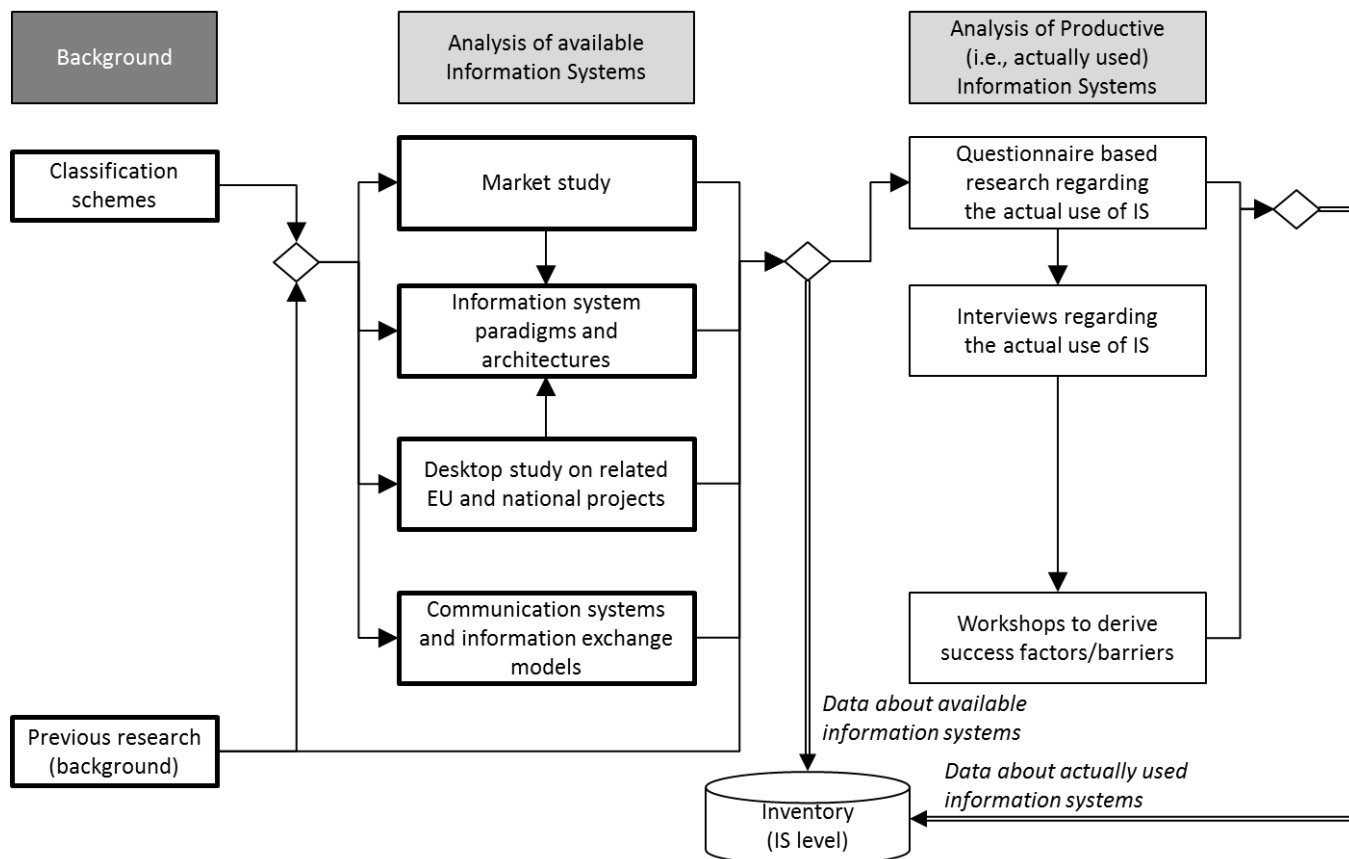


Figure 14: Current status of activities in task T3.3

Analysis of information was conducted as follows:

- Implementation of **Market** and **Desktop studies** for performing an ongoing study on information systems: In order to extend the overview of information system on basis of SecInCoRe background, further available applications on the market were collected and analysed. To include the scientific efforts in this area, national and EU projects were researched on. On basis of these both approaches the industrial as well as the research landscape can be brought together enabling a comprehensive analysis.
- Analysis of **communication and information systems**: Based on the research studies from the market analysis structures and categorisation of information system were defined in SecInCoRe. The ongoing extension of the amount of



information system show the validity of the categorisation. Besides the structure of information systems the interfaces to other systems is also important. For that purpose, communication systems are also important. Thus the search and analysis of respective systems, their characteristics and architectures was in focus in the SecInCoRe inventory.

- To discover information systems actually used, the EPISECC questionnaire was used to identify relevant information systems in use from some of our Advisory Board members: e.g. partners from the Lancashire Resilience Forum were asked especially having the UK national system 'Resilience Direct' in mind.
- Another research aspect was **success factors** for the uptake of information and communication systems. First insights and frameworks are presented based on literature research and inspection. Further these results are also reflected based on the overall inventory and related demonstration cases in the validation of the knowledge base.

4.2 Structure and Acquisition of Information systems

The structure based on results presented in D3.3 was approved by the ongoing gathering of further available information system, the categorisation of these systems and the inclusion in the respective SecInCoRe database. The scheme is shown in Figure 15 below.

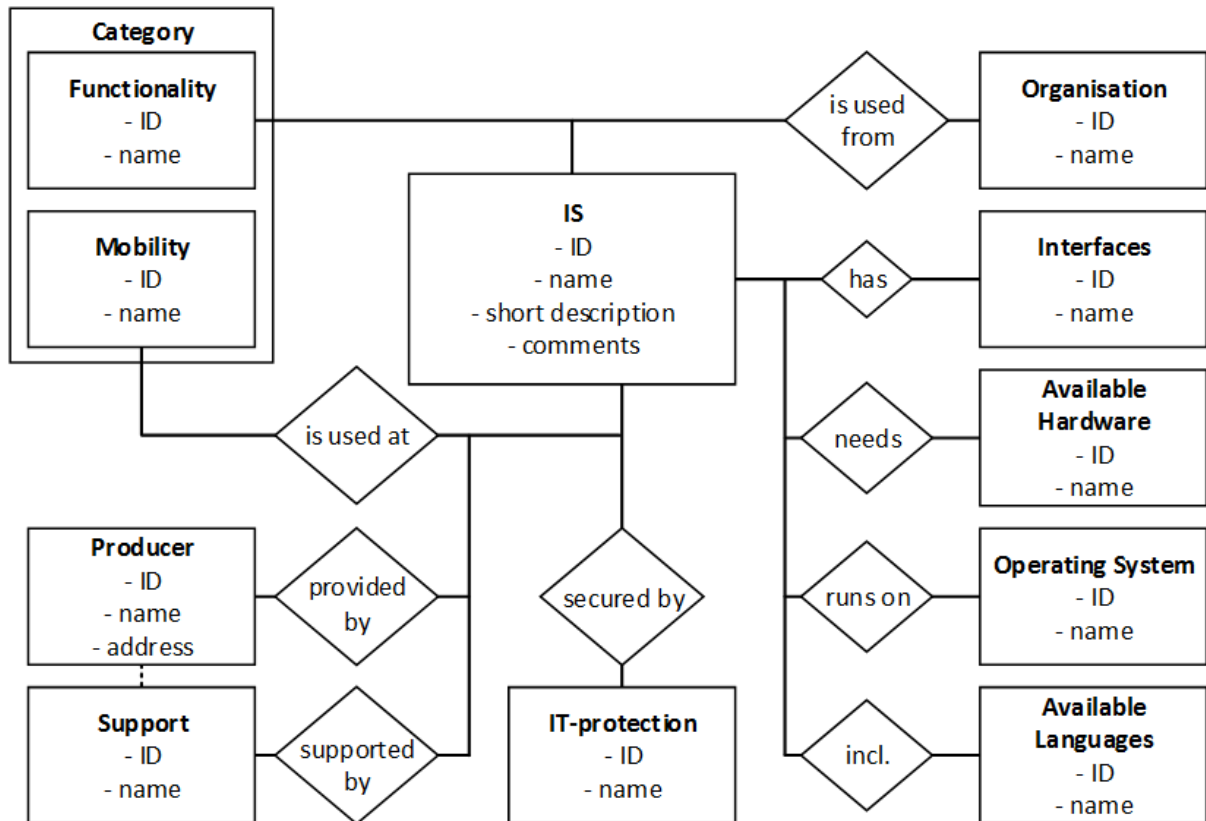


Figure 15: Database scheme for information systems (see D3.3)

The number of systems by category is presented in the following Figure. The process for the identification of the categories was already presented in D3.3. In total there are 125 system gathered and stored in the information system database.

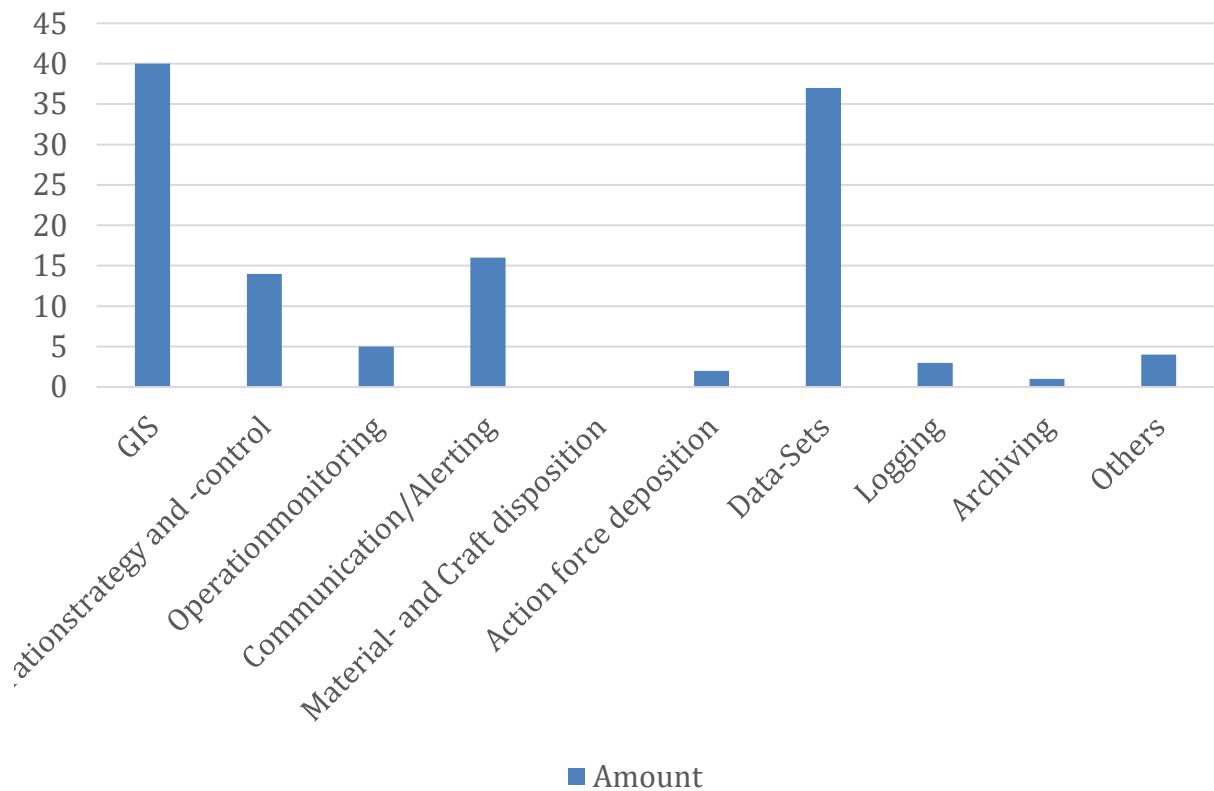


Figure 16: Number of systems gathered in each category

One aim was to highlight the categorisation of system and defining a model to describe information system used in emergency situations. A further aim was to represent as many countries as possible in the study of available information systems. The EU spread is demonstrated in Figure 17.

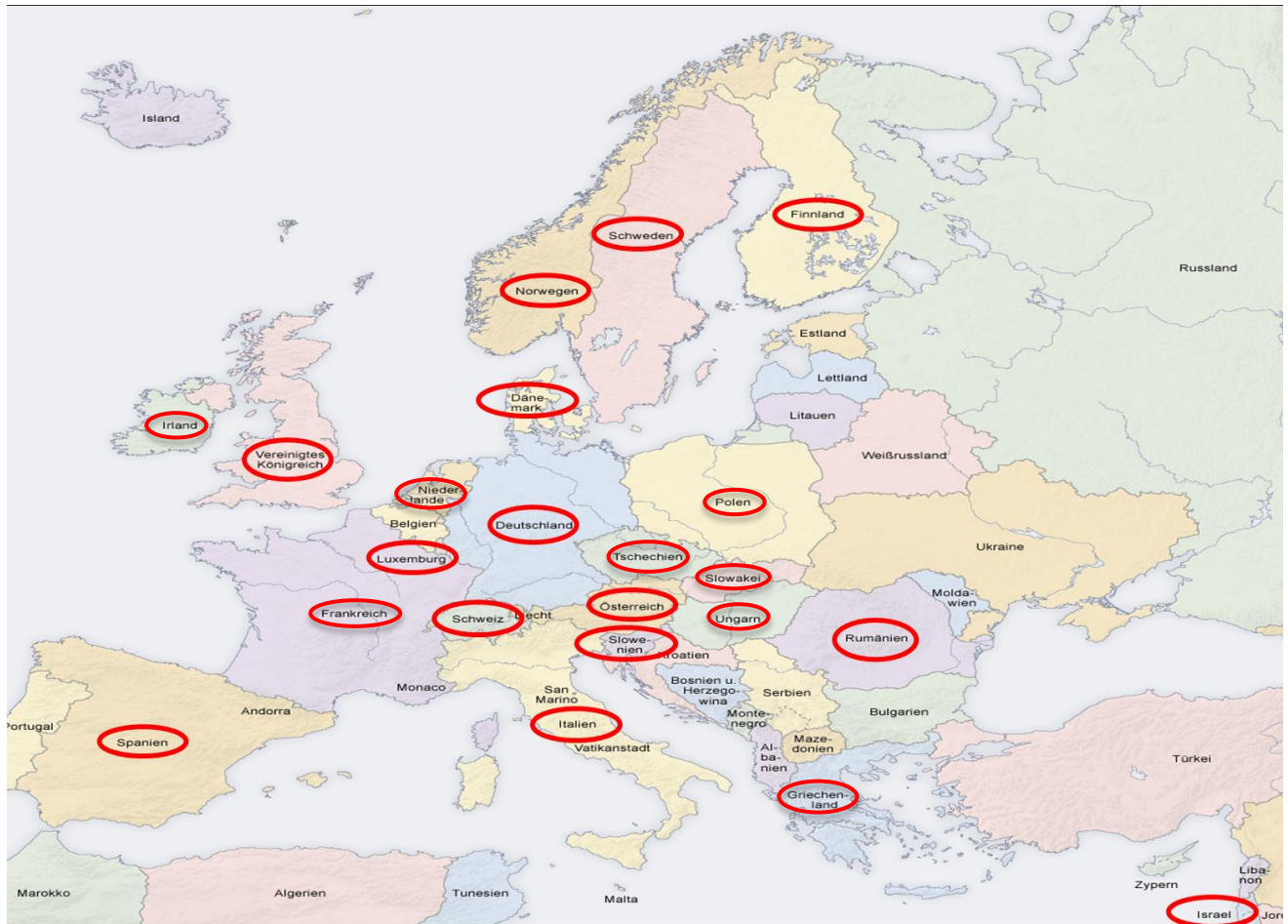


Figure 17: Spreading of gathered information systems in the SecInCoRe Knowledge Base

Based on the described approach, the database was setup and used to store all gathered information systems.



InformationSystems		App Framework				15:33:4
ID INT(11)	Country TEXT	Title TEXT	Short_Description TEXT	Gateways TEXT	Available_Hardware TEXT	Available_Languages TEXT
66	Germany	CEBOS 2000 GIS-3D	Clear visualization of vehicle locations, symbols and incidents.			
67	Germany	NORUMAT 4000	Efficient and effective use of action forces.			
68	Denmark	ARGOS	ARGOS is a software system to support the emergency organization to make the best possible decisions in case of			
69	Germany	UMWLS	Integrated control system for environmental monitoring and civil protection			
70	Germany	FeWIS (Wetterinfor...	Weather forecast and severe weather warning.			
71	Germany	GeoFES	Situation exploration and spatial analysis			
72	Sweden	Carmenta CoordCo...	Call takers and dispatchers can control and coordinate the entire chain of emergency or incident events.			
73	Sweden	Carmenta RisQMap	Multi-user map display designed to be used in mission critical applications, such as Public Safety and National Se			
74	Spain	SiCom Suite	Enables any NG 911/112 Center to make effective decisions, based on comprehensive, accurate and real-time in			
75	Italy	emma (emergency ...	Solution to build Command and Control Center of the Fire Department.			
76	Germany	eCall	Ensures that the rescue forces are notified about incidents more quickly.			
77	Germany	AVIOTEC	Uses Intelligent Video Analysis to detect smoke and flames.			
78	United King...	LocationWise	Delivering highly accurate mobile location data.			
79	Canada	FDM RMS	Solution for data capture and reporting used in the Fire and EMS industry.			
80	Canada	FDM CAD	Fully integrated, real-time mapping and data entry system that allows Fire and Emergency Service agencies to pri			
81	Canada	FDM GIS Analyst (G...	Provides the analyst and decision-maker with real-time RMS and CAD data for better decision-making.			
82	United States	Fire RMS	Fire Records management solution to manage the daily operations and reporting requirements for Fire Departm			
83	United States	Fire Forms Fast (F3)	Developed for use in volunteer, municipal and other governmental fire departments.			
84	United States	ESP Incident Repor...	Additional reporting functions can be integrated right into the NFIRS 5.0 reporting structure.			
85	United States	DataForce Web	Professional Fire Reports software solution with high quality, functionality and flexibility.			

4.3 Success factors and barriers for the uptake of information systems

Figure 18 Database implementation

Another main part of the research work conducted in T3.3, was the identification of success factors and barriers in the uptake of information systems.

4.3.1 Definition of success factors

Moreover, one goal of SecInCoRe is to find new or modify existing business models for IT-systems in Public Safety and Security. Therefore, success factors have to be identified to create a basis for new business model concepts. The most effective analysis of critical success factors is done top down [York88]. SecInCoRe's approach was to find critical success factors that are necessary to be successful for information system provider but in the same time also for the user of these systems in Europe. Afterwards specific success factors could be defined for specific countries.

4.3.2 Interactions between basic success factors from an IS providers and IS users point of view

For defining success factors a two-step approach was followed. First, a literature review of existing approaches was taken into account. Second, the previously defined Key Performance Areas (KPA) were analysed with regard to success factors.

The SecInCoRe consortium defined four KPA in [3]. These KPAs are part of the validation strategy of the SecInCoRe outcomes. In order to define criteria regarding the success factors of the use of IS, the KPAs were taken into account:

- **Operational Procedures (OP)** – in this context operational procedures are meant:
 - a) The development process of IS provider
 - b) The process of use and moreover the quality of use and the integration in existing FR – processes (like command and control)
- **Efficiency (E)** – measurement of factors of efficiency of IS and further the efficiency of FR operation due to the use of IS
- **Capacity (C)** – range of function and capacity of IS and in this relation the capacity of FR organisations
- **Economic considerations (EC)** – in this KPA aspects like the IS provider's sales rate as well as procurement regulations and opportunities of FR organisations are grouped.

Based on research outcomes of SecInCoRe the importance of addressing ELSI in system design process lead to one more KPA:

- **ELSI viability (EV)** – security, availability, reliability

Moreover literature research ([MBP04], [Dorn94]) expose further KPAs directly linked to the use case of IS-provider and the respective user.

In D3.3 a first overview over basic success factors regarding IS providers and IS user was given (see figure below). Further a relation to defined KPAs in relation to [3] are given.

IS-Provider	IS-User
Support by executive board (EC, OP)	Revise false expectations (C, OP, EV)
Involvement of end users (C, OP, E)	Thinking as a whole, starting with parts (OP)
Experienced project managers (EC, OP)	Promotion by leadership, acceptance of everyone (OP)
Distinct business goals (OP, EC)	Quality not quantity of information €
Straightforwardness (OP, EC)	Including external information (E, OP, C, EV)
Standardised software infrastructure (EC, OP)	Consistency of data (EV, E)
Stability of main requirements (OP, EV, C)	User-friendly display of information (OP, C, E, EV)

Reasonable process model for the whole software lifecycle (OP, EC)	Connection to other applications (C)
Reliable calculations (EC)	Flexibility and dynamic (OP, C, E, EV)
Motivated and competent team (OP, EC)	

Figure 19: Basic success factors by [Dorn94] and [MBP04]

What becomes obvious is the distinction between provider and user and therefore, between KPAs targeting the economic impact of IT system development and the KPAs more related to functionality and efficiency of a system.

In a next step these success factors were analysed in more detail regarding the interactions between the IS-providers success factors and the IS-users. The result can be seen in Figure 20.

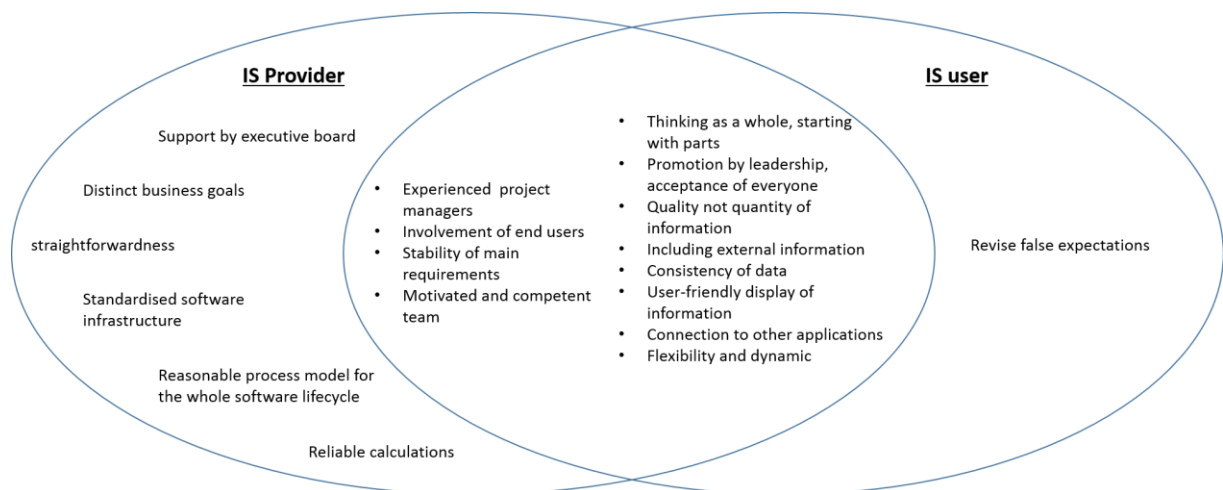


Figure 20: Overlapping of success factors targeting provider and users

The figure shows, that only four success factors of the IS providers point of view are actually having an impact on that of the IS-users. To give a better overview over the interactions they were displayed in following Figures.

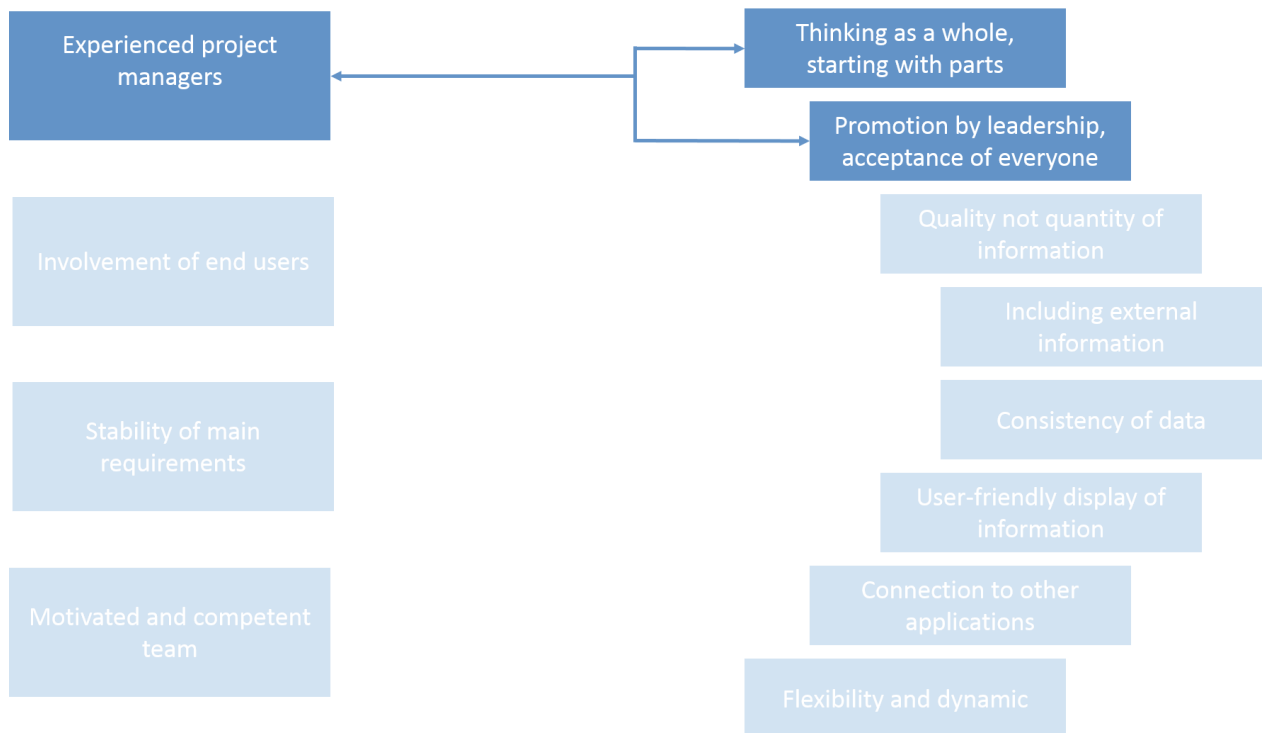


Figure 21: Influence of experienced project managers on IS users SF

Experienced project managers have a good understanding of a projects complexity. Complex projects should start in with basic features and should be introduced within the company in a small department [SG01]. The project manager knows a project's goal and how to accomplish it. The experienced project manager can support the leadership and new users/workers in promoting the new IT-system, related social practices, and convince critical employees. This situation is adaptable for introducing IT-system in first responder and Police Authority organisations.

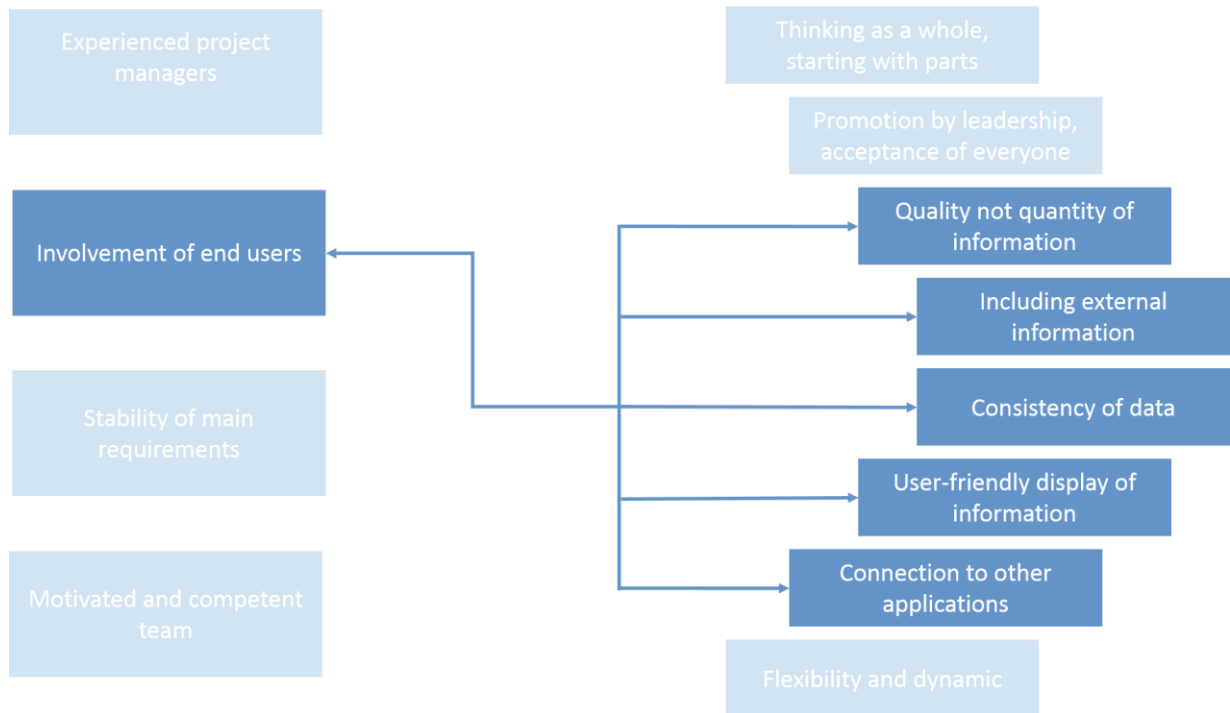


Figure 22: Influence of involved end-users on IS users SF

To gather the needs of end-users they need to be involved into the development process. This way developer knows which end-user needs which information and therefore, is able to develop a user-friendly system with a high quality of information, even taking external information in consideration, if needed. To use the results of the developed IT-system in other applications the developer needs to know which applications need to be integrated. There are several methods existing to ensure the integration of end user in the developing process. Used method in SecInCoRe was the 'collaborative-design' described especially in research results from WP2.

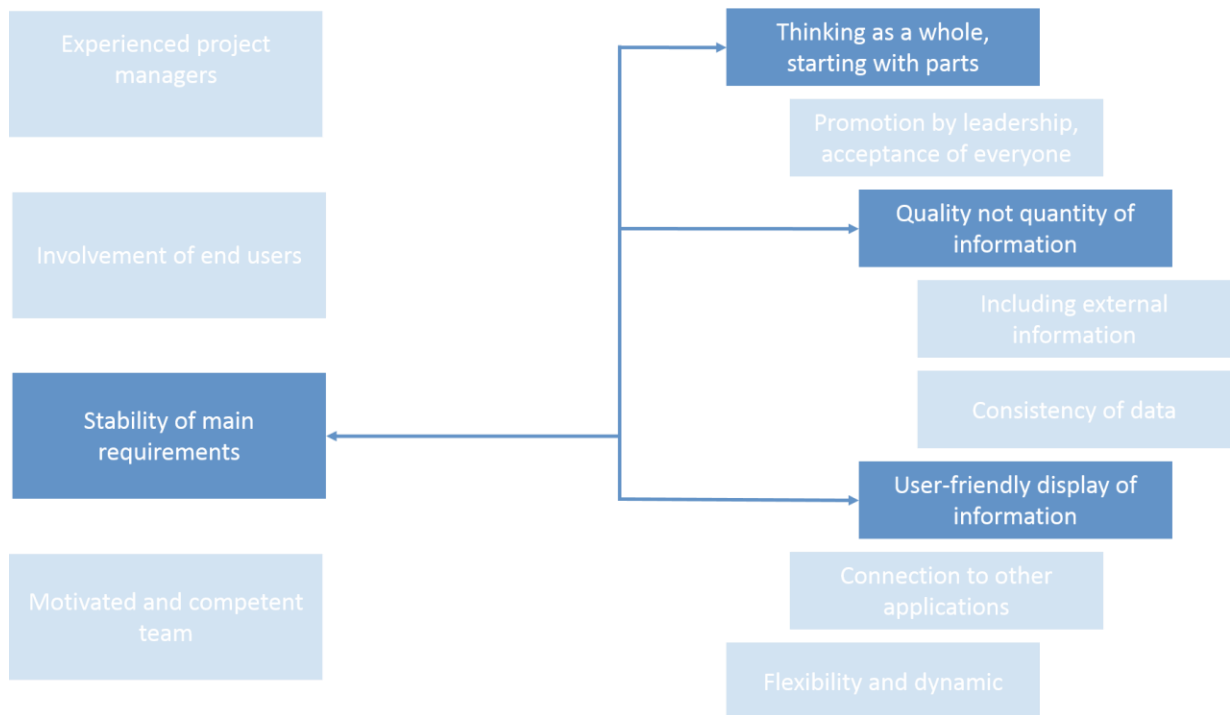


Figure 23: Influence of stable main requirements on IS users SF

Defining main requirements and developing key features to fulfil these requirements helped to keep the straightforwardness which covers the SF: "thinking as a whole, starting with parts". The development of more advanced features is successful only if key features can be successfully implemented in the company's system. This has also a direct impact on the quality of information that IS-users get. Key information need to be displayed to support the end-user, as opposed to large masses of detail which prevents the user from getting a clear overview.

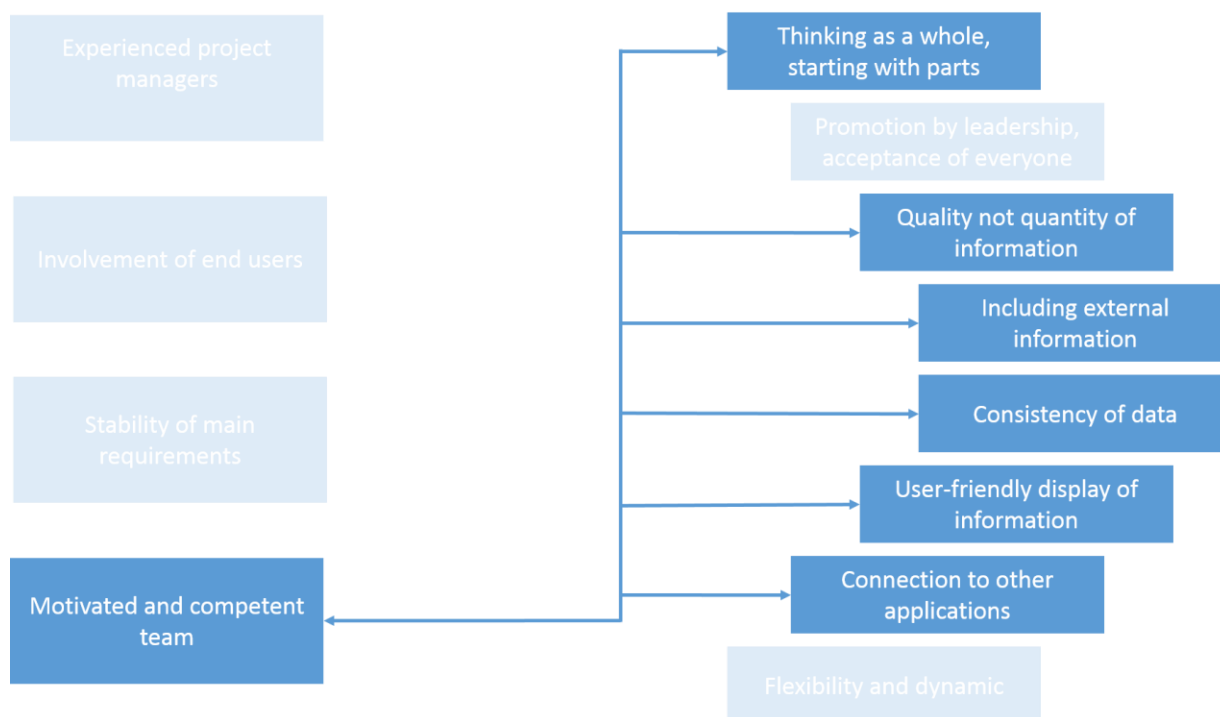


Figure 24: Influence of a motivated and competent team on IS users SF

A well-rounded, highly motivated and competent team are the main requirement to support an experienced project manager. They know how to reach the goals the project managers defines, how to solve problems in the development process and with the end-users.

4.3.3 New success factors based on failed projects in Germany

To identify CSFs for Europe regarding IT-systems in the public safety and security sector the first approach was to identify failed projects in the public sector in Germany with internet research and literature inspection. This lead to overall 16 projects. Computerwoche.de listed 10 failed projects [www3], Spiegel.de listed 9 failed projects [www4] and Mertens analysed 7 failed projects in Germany [Mert09]. While very specific problems occurred in these projects, it was able to identify general reasons that happened in multiple projects across the public sector. The main reasons for these 16 failed projects are:

1. Misinterpretation of task complexity
2. No definition of the task leader / wrong project management by public authority
3. No exact definition of the task itself
4. Lack of communication (provider – authority, provider – end user, authority – end user)
5. Wrong risk management
6. Politics (could fit into 2) but its more diverse than just a task leader / project management decision)

Results of the problems were:

- 1.



- a. Delay of project
 - b. promised functions didn't work
 - c. not enough workers
 - d. too many parties involved
- 2.
- a. No person in charge to make the final call <-> too many parties want to make it their way -> discussions instead of progress;
 - b. no responsibilities for mistakes <-> no one cares if projects fails, because it's not their fault
 - c. cost explosion
- 3.
- a. Provider interprets the task as they want
 - b. Increased complexity
 - c. No proper technical solution
- 4.
- a. Authority orders software which isn't needed
 - b. Provider develops tools, which will not be used by end users
 - c. Software is too complex
 - d. Software doesn't cover the functions it should
- 5.
- a. No risk management for miss calculations (cost / time)
 - b. Issues are not / too late communicated (no control system)
- 6.
- a. Too many parties involved forcing too much discussions leading into 2) & 3)
 - b. See also topics at 4.

In a next step the reasons listed above are compared with the main success factors for IT-projects in order to learn about the main reasons of project failure:

1. Misinterpretation of task complexity:

The first reason is covered by multiple success factors defined by [MBP04]. At first experienced project managers are a key reason for the success of IT-projects. An experienced project manager has a general understanding of requirements of speciality departments and software engineering as well as experience in organisation and leadership. Straightforwardness is the second success factor relating this topic. The larger and more complex an IT-project is, the higher is the risk of failing as it gets more difficult to handle.

2. No definition of a task leader / wrong project management by the public authority:

As listed in the results the absence of an official task leader of the public authority can lead to big discussions within the organisation and the IS provider can't solve problems occurring efficiently. If there is no person responsible for the failure of the project no one cares about the failure. None of these reasons are covered by the standard success factors as the public authority can be seen as a third party



in this kind of problem. Therefore, every stakeholder has to announce a person in charge to make final calls.

3. No exact definition of the task itself:

The stability of the main requirements has to be ensured. The main requirements have to be defined to cover the central functions of the project. Based on these, following levels are developed but should also allow flexibility in the definition of the requirements keeping the high-level requirements untouched. To prevent the misinterpretation of tasks the IS provider has to involve end users as well. Otherwise the provider will risk to fulfil the major requirements of the project. End users have to be involved in a responsible position for the specification, acceptance and user organisation within the development process.

4. Lack of communication:

This reason is covered partly. The lack of communication can be solved by involving end users. But as seen in the results of the problems the lack of communication isn't solved by only communicating on the developer – end-user level. Public authorities can order new IT systems which aren't needed. To solve this problem a communication channel between all parties has to be set up using a common terminology ensuring understanding between each other.

5. Wrong risk management:

A solid risk management is a key factor to solve occurring problems. A reasonable process model for the whole software lifecycle can help from the IS providers point of view. But there has to be an efficient process within the public authority as well, as the project will probably cost more money and/or take more time than planned. Quality gates have to be defined in cooperation with all involved parties to explore upcoming problems early and efficient.

6. Politics:

The larger a project gets, the more stakeholders are involved. This usually leads to frictions between those as the stakeholders serve their interests. This isn't an IS provider nor an IS user kind of problem. As there will always be projects where stakeholders are dependent on each other (e.g. government vs. parliament). There is not really a solution that could be defined as a success factor to prevent problems occurring around politics.

To summarise, the following old and new success factors cover the main reasons for failed projects:

- Experienced project managers (old)
- Straightforwardness (old)
- Stability of the main requirements (old)



- Involvement of end users (old)
- A reasonable process model for the whole lifecycle (old)
- Definition of a main person in charge for all stakeholders (new)
- Set up of communication channel between all stakeholders (new)
- Definition of quality gates for all stakeholders (new)

Based on these results related to the analysis of success factors the analysis conducted to derive conclusion on existing and used business models will follow in the next section.

5 Business models for the application of information systems

As defined in previous deliverables, one of the tasks of WP3 is dedicated to the analysis of business models for the sustainability of information systems.

5.1 General approach to define business models

The followed approach for the analysis is explained in Figure 25. Through a dedicated review and analysis of current laws and procurement directives, in addition to procurement guidelines, the main process to obtain information systems by emergency services was performed. Or, the other way around, a further step, in addition to the current laws and directive, has been dedicated to the investigation of information systems somehow similar to the one of SecInCoRe in order to analyse the business models they use. Results have been collected in the Knowledge Base dedicated to business models¹. The aim of the current chapter is to describe the state of the art of the gathered business models and to share the analysis based on the sources stored in the Knowledge Base.

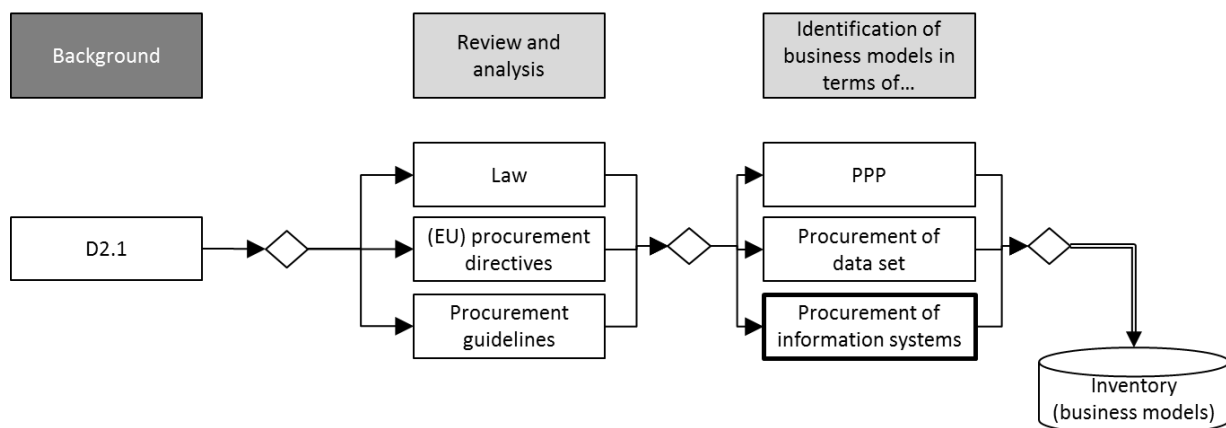


Figure 25: Research approach for the analysis of business models

5.2 Definition of the main relevant models of business

Through the literature review and desk analysis, it has been possible to identify some crucial points when talking about business models for information systems for emergency services. The main finding is related to the perspective that is adopted to face a discussion on business models; it has to be considered who has to buy or to obtain an information system, and, on the other side, the operated business models by those who are implementing and promoting an information system.

Starting from the perspective of national emergency services, being generally public institutions, which intend to adopt an information system it is generally necessary to follow the rules of public procurement. For this reason, a first work of analysis was dedicated to public procurement procedures in various European countries. What emerged is that public procurement can change from country to country, even if in Europe the process has been harmonised compared to the past in order to align

¹ Knowledge Base on Business models is available here
<http://31.171.245.222/sqlbuddy/#page=browse&db=BusinessModels&table=Businessmodels&topTabSet=2>



procedures. In addition to public procurement other forms, such as public private partnership are also applied.

On the other hand, if we adopt the perspective of who implements and sells information systems, different business models can be developed. The variety of business models depends on the different approaches on which the information systems are based, on the different scopes and also to the different actors that implement the system.

In line with this, the data gathering about business models for the KB has been performed in order to identify the most relevant business models for information systems used by emergency services for crisis management. With this it has been possible to identify four major business models that are adopted for information services. Such models have also been discussed with the users that attended the SecInCoRe workshops in order to verify the correctness of the categories. The four models identified have been categorised as following:

- publically funded Pan-EU model;
- vertical model, that can be public or private, focused on specific emergency or related topics;
- not-for profit model, building a volunteer community, that could be a new community or integrating outcomes into an existing one;
- commercial model based on private companies.

Clearly, some business models might have overlaps between those categories or they do not fit perfectly. However, a categorisation was needed to allow the analysis of the information stored in the KB. A short description of each category is given in the next paragraphs to better understand the following analysis and was derived from the results of the second AB-meeting in Athens.

The publicly-funded Pan-European Model is based on the investigation of several information systems that are provided and maintained by European institutions or national governments interested at a European scale. This model implies that European institutions, or national ones, develop and maintain a system that can be used by other single institutions. An example² of this kind of model is provided by Eurodac (European Dactyloscopy), a fingerprint system developed by the European Commission for asylum-seekers and those who cross borders by irregular means purposes and other systems. Other can be:

- VISI II;
- PolOnline.

This kind of model shows several positive aspects: first of all, it has the highest level of trust due to the fact that it is under the control of an established institution. Furthermore, due to the property of a European body the maintenance of the system is guaranteed through public funding.

The second model is related to the information systems that are based on a vertical implementation. This means that there are information systems which very much focus on a single topic. For example, Chemdata, is one of the most trusted sources of information in its sector providing information only on Chemical incidents. This type of

² All examples inserted in Chapter 5 are also available in the dedicated Knowledge Base.



information systems can be public or private; the business model is built on the specific level of information the system can provide and they are generally based on a pay-per-use system or based on an annual fee. For example, in the case of the Interpol crimes database, the business model is based on a pay-per-use solution: each country pays according to the number of searches done by its own agents. Another example is the Hazchem database for chemical emergency which is managed by a private company, Herwell, UK. This database is run on a fee basis for all stakeholders that want to access the database.

In the case of a vertical implementation, information system can be provided and hosted by a public actor as well as by a private company; what is an important outcome of the analysis is that users pay for the detailed level of the information.

The third business model is based on approaches developed by not for profit organisations. In this sense, no profit organisations and consortia develop free and open-source solutions that can be used for free by the stakeholders for the benefit of the entire community. Examples for this category are rather rare, a main example is Ushahidi³. Ushahidi (Swahili for "testimony" or "witness") is a web application created in the aftermath of Kenya's disputed 2007 presidential election that collected eyewitness reports of violence by volunteers. These were sent by email or text-message and were mapped on a Google map. The model adopted by Ushahidi is based on the fact that the app is free". In addition one of the founders, Mr. Hersman, clarified in an interview⁴ that the company prefers not to take any public funding from any country in order to maintain its neutrality on the provided data. Always following Hersman's statement, Ushahidi's primary source of income is a private foundation grant funding (e.g., Omidyar Network, Hivos, MacArthur, Google, Cisco, Knight, Rockefeller, Ford), however there are on-

³ In 2008, Ushahidi, Inc. was founded. This is a non-profit software company that develops free and open-source software (LGPL) for information collection, visualisation, and interactive mapping. Ushahidi (now one of the company's products), which has since been improved, released freely, and used for a number of similar projects around the globe. Now in its 3rd version Ushahidi v3, The Ushahidi Platform (which will have both an open source and a cloud version) has grown from a crisis mapping tool to a management platform for crowdsourced data. According to the link <http://mediashift.org/2012/08/whats-next-for-ushahidi-and-its-platform226/> "The purpose of v3 is to provide a better crowdsourcing platform, so that the leaders, crisis responders, funders, and decision making organisations can do their work more efficiently, gather better information, and understand what's happening on the ground". According to Hersman, "Ushahidi is used in over 150 countries, it has been translated into 35 languages and has been deployed over 40,000 times. From earthquakes in Haiti and Japan, to floods in Pakistan, blizzards in the US, fires in Russia and elections in East Africa and South America. Ushahidi has been used by individuals, civil society groups and governments. [...] Ushahidi has also been widely used by funders to governments as a way to gather information to improve decision making".

⁴ Interview is available here <http://mediashift.org/2012/08/whats-next-for-ushahidi-and-its-platform226/>



going efforts to diversify funding with earned revenue from client projects. Other examples for this category are:

- Ready;
- Disaster Recovery.

Examples, as the ones reported above, show that generally no profit models are based on the volunteer will of organisations to make information and data available for free. This type of information systems can be based on crowdsourced information, as in the case of Ushaidi, or on the owner of the system, as in the case of Ready which is sustained by the Department of Homeland Security of the United States. In all cases, the not-for-profit model is generally open source and publically available.

The last identified business model type is related to a proper commercial strategy that implies the selling for profit of a service or product useful for crisis management. This kind of business model is very often used by private companies developing solutions for emergency services. Some examples are:

Cisco;

- Eagle Crisis Management Suite;
- Hegeo;
- SIS EmerGeo.

These examples are current private commercial disaster databases or crisis management systems provided by private societies, selling their product or solutions. Other important examples to take into account are Google or Microsoft. The commercial model is generally followed by private companies that develop solutions for emergency that can be used by stakeholders according to the price they pay for the solutions. Such solutions are generally modular, namely based on different components that can be bought separately and also integrated with other existing technologies.

5.3 Report on the Business Model Inventory

The KB is an important tool of the SecInCoRe project that should be continuously improved by adding new contents and sources. At the moment of the writing, and as reported in Figure 26, the Knowledge Base on business models contains 70 entries.



se (70) Structure Insert Query Import Export			
All None With selected: Edit Delete Refresh			
ID	title	description	source
0	Guidelines for Business Model Inventory	Within the activities of SecInCoRe, WP3 promotes the	SecInCoRe D3.2-D3.3-D6.1-D6.2
1	EURODAC	EURODAC is a systems that is under the umbrella of a	http://ec.europa.eu/dgs/home-affairs/what-we-
2	SIS	System SIS (managed by the SIRENE agency) for	http://ec.europa.eu/dgs/home-affairs/what-we-
3	HAZCHEM	Hazchem (for chemical-related emergency) managed by	https://en.wikipedia.org/wiki/Hazchem
4	USHAIDI	Ushahidi (Swahili for "testimony" or "witness") is a we	https://www.ushahidi.com/
5	European Incident Command System	ICS data for fire services on www.f-e-u.org provides	http://www.f-e-u.org/ics.php
6	NatCatSERVICE	Comprising some 37,000 data records, NatCatSERVICE	https://www.munichre.com/en/reinsurance/business/non-
7	CatNet®	wiss Re offers clients a range of proprietary tools	http://www.swissre.com/clients/client_tools/about_catnet.f
8	Visa Information System	The Visa Information System (VIS) allows Schengen	http://ec.europa.eu/dgs/home-affairs/what-we-
9	European Health for all databases (HFA-DB)	HFA-DB provides a selection of core health statistics	http://www.euro.who.int/en/data-and-
10	European detailed mortality database (DMDB)	DMDB was developed in 2007 to provide user-friendly	http://www.euro.who.int/en/data-and-
11	Tobacco Control Database	The database illustrates the leading countries in the full	http://data.euro.who.int/tobacco/
12	Centralized information system for infectious diseases	CISID presents the incidence of infectious diseases	http://data.euro.who.int/cisid/
13	Advice and Information Management System (AIMS)	A database and information management system for	http://www.lasa.org.uk/aims/
14	Chemdata	Chemdata is a chemical hazard database containing	http://the-ncec.com/
15	Incident control room	Incident Command software designed to support the	http://www.incidentcontrolroom.com/
16	Stolen and Lost Travel Documents (SLTD)	The ?SLTD database contains records on lost, stolen	http://www.interpol.int/INTERPOL-expertise/Border-
17	Stolen Administrative Documents (SAD)	The SAD database records stolen official documents	http://www.interpol.int/INTERPOL-expertise/Databases
18	Stolen Motor Vehicle Database	The INTERPOL Stolen Motor Vehicle (SMV) database is	http://www.interpol.int/Crime-areas/Vehicle-
19	DNA database	Police in member countries can submit a DNA profile	http://www.interpol.int/INTERPOL-
20	Europol Information system (EIS)	The main objective of the Europol Information System	https://www.europol.europa.eu/content/page/europol-
21	144 Niederösterreich	Niederösterreich provides an example of how an	https://www.144.at/homepage/startseite.html
22	Italy	The Public procurement legislation in Italy has been	SecInCoRe D6.1
23	France	According to Article 1 of the Code des Marchés Publics	SecInCoRe D6.1

Figure 26: Knowledge Base on Business Models

The database, that forms the basis for the KB, is structured in a way that each entry has the following fields: Id, title, description, source, language, country, publisher and category. The structure of the database is shown in the Figure below.

Businessmodels ▼	
ID INT(11)	
title TEXT	
description TEXT	
source TEXT	
language TEXT	
country TEXT	
publisher TEXT	
category TEXT	
Version INT(11)	
timestamp TIMESTAMP	
Indexes ▼	
PRIMARY	

Figure 27 Structure of the business models database

As said, entries have been collected starting from a research based mainly on desk analysis and information gathered from stakeholders. Through the search, it was possible to identify systems which were relevant from the point of the contents or

functioning for SecInCoRe and where it was possible to identify the used business model.

The entire database is constituted according to the categories reported in the following Figure 28.

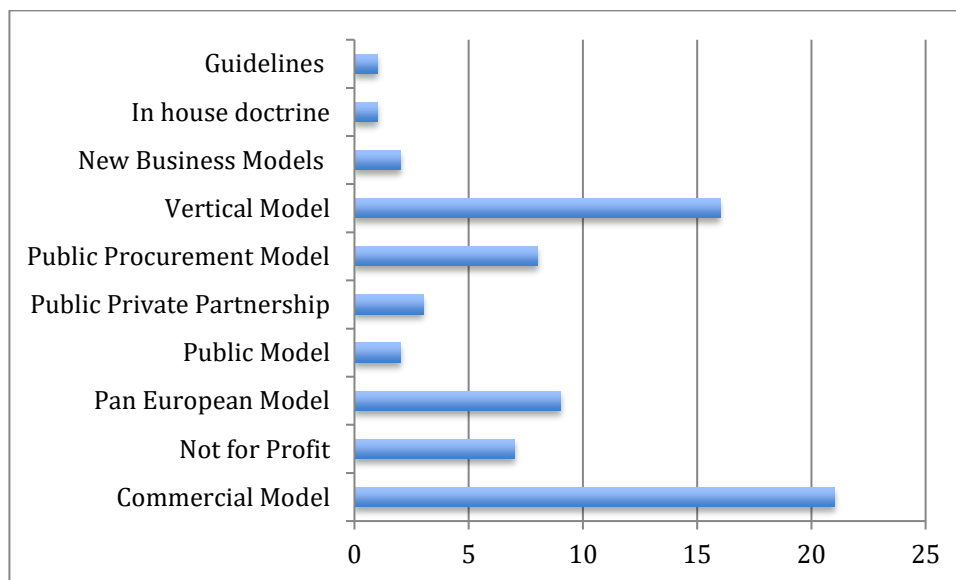


Figure 28: Report on the included Business Models in the Knowledge Base

In addition to the information on the four models of business that have been introduced already, also other information has been stored due to the fact that they cover other aspects related to business models that have been analysed under WP3 and WP6. In particular the database contains:

- A guideline to explain the way in which the data gathering has been performed;
- Information on Public Models that are not related to European countries (and that cannot be defined as Pan European);
- Examples of Public Private Partnerships;
- Examples of Public Procurement Models from European countries;
- Information on New Business Models;
- Information about in house doctrine.

These kinds of sources have been taken into account as complementary information to the analysis of business models performed during the project lifetime and for this reason they have been stored in the KB. In particular, this material was relevant in an early stage of project development during the investigation of procurement systems from public authorities or on other kinds of procurement that can be implemented in regard to new business models or in house development.

However, the information related to business models that are much more relevant for the scope of this deliverable is reported in Figure 29 and is related to the above described four categories.

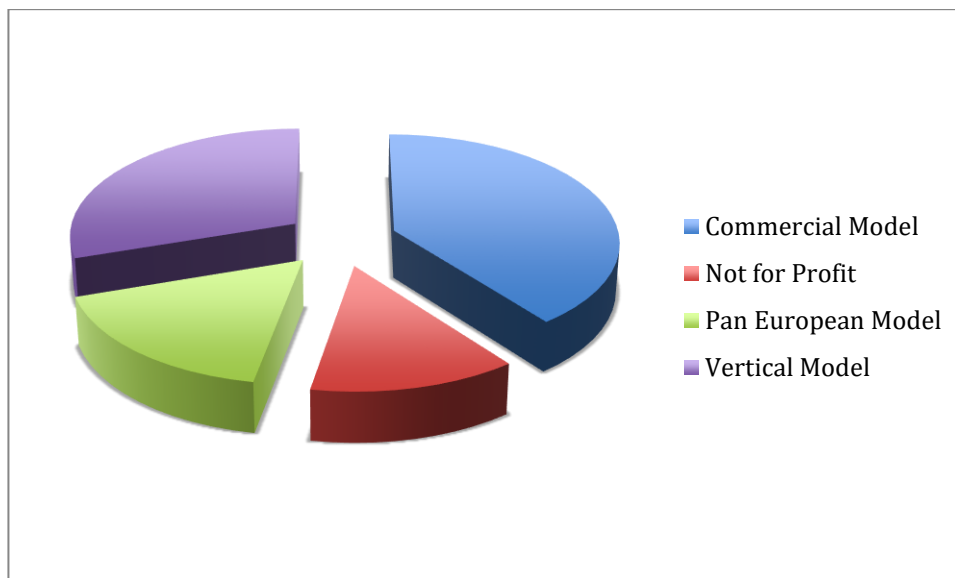


Figure 29: Report on the main for Business Models identified

As reported in the Figure, the majority of information is related to the commercial model (with a total of 21 sources) and to the vertical one (16 inputs). Less populated are the categories about a publically funded Pan European model (for a total of 9) and Not for Profit (with 7 examples).

Observing the critical mass of information stored it is possible to notice that 69 entries out of 70 have been retrieved and collected in English, the only one that is not in English is in German.

For 100% of the entries in the KB a brief description is provided; in addition, there is a link to the primary source in order to retrace where the information came from. Indeed, 14 entries are related to documentation stored in other deliverables produced by SecInCoRe, while the remaining 56 sources are connected to proper links and websites available on the Internet.

Regarding the geographic distribution of the gathered information, it was not always possible to identify the country to which the investigated information system is linked. However, it can be said that more than 50% of the information is related to information systems connected to European countries. In addition, in order to allow some comparison and to enlarge a bit the field of investigation, some examples of information systems have been included which were developed outside Europe. This enables the possiblitiy to find also interesting approaches from outside Europe.

- 4 examples from United States;
- 2 from Canada;
- 1 from Kenya;
- 1 form India.

5.4 Analysis of existing business models

The data gathering of business models related to information systems performed during the project lifetime opens some points of reflection. The analysis provided in this



paragraph aims on one hand to help the reader in a better understanding of the information collected and stored in the KB, on the other hand wishes to improve the comprehension of the business models in a such a complex environment as crisis management and security.

Looking at the way in which companies, institutions and organisations have organised and built their own business in relation to information systems for crisis management, it is evident that the primary distinction that exists in terms of business models is between publically funded systems and private ones. In this sense, the publically funded model can be further divided. Such model can be identified at European scale, as most of the examples provided in the KB, and for this reason called Pan-European, or at a wider scale, such as the examples of information systems provided by international organisations, as in the case of systems developed by the United Nations with the support of other high-level actors (e.g. the Global Disaster Alert and Coordination System).

In the case of publically funded models, such systems can be the result of an internal effort (e.g. EDRIS) or the result or further development of project's outputs that have been somehow adopted by European institutions. For example, it is not uncommon that results from European funded projects have been supported and then implemented by European Institutions and related agencies becoming live platforms. The result is that such instruments are in most of the cases open to public use or to selected users.

On the other side, the approach adopted under the defined commercial model is generally pursued by private companies that internally develop concepts, technologies or knowledge. Such products or services can be bought by anyone interested. In the majority of these cases, private companies developed modular solutions allowing buyers to decide which component they want to buy. Singular components can also be applied and integrated to other existing solutions. Payments can be either done by paying per use or through tailored options that depend on what the user is buying and in which version. This case is represented by Crisis Commander Ltd which is a privately owned Swedish company developing cloud-based crisis and incident management software or by C4i, based in Canada, selling interactive, electronic tablets for training solutions for emergency response and crisis rehearsal training, designed specifically for Emergency Management staff, Emergency Operations Centres and Civil Leadership.

In this latter case it emerges that the customers of private solutions can be very wide, from private buyers to public ones. In the case of private ones, the main ways to sell products and solutions are pay per use or based on annual fees. In the case of public buyers, even private companies have to follow the rules of public procurement to sell their solutions.

Another aspect of the analysis shows the high number of private companies that develop and sell information systems for crisis management in comparison to publically funded solutions. During the investigation it also emerged that a high number of companies in the field are based in the United States. However, due to the relevance of European based solutions, only some examples of US companies have been included in the KB.

In addition to the two categories presented so far, a cross cutting category emerges from the analysis that has been defined as vertical model. As already written above, the reason behind the definition of such category is due to the fact that the business model is in this case built on the specificity of the solution or knowledge provided. This



approach is generally followed by public institutions (e.g. Interpol or WHO) but it can also be characterised by a more business-oriented strategy. This means that in some cases the access to the system is not free of charge but can be subject to payment conditions. This approach highlights that the line between a business model based on profit or on not-for-profit cannot be totally dependent on who has the property of the information system because sometimes who should be seen as a public actor and mostly recognised as a developer of free solutions or knowledge is not.

The final category that has been analysed is the not-for-profit model. Under this category several examples have been collected that show how systems, which are similar to SecInCoRe, have been implemented by not-for-profit organisations, institutions or even companies, just for the general well-being and safety of people. In cases such as 'Ready' (<https://www.ready.gov/>), guidelines for preparedness for storms are updated directly from the US government for the citizens. Examples such as Ushaidi, DMIS or Open MRS Wiki, on the other side, are provided by not-for-profit organisations. In both cases, these examples give a wide space of reflection on the importance of building a community and sharing technology and information with citizens for the entire society and how information systems based on open source solution can really make the difference for the common welfare.

Summarising, the largest number of sources that have been collected on information systems are based on business models made with a proper commercial scope, which can be sustained by private companies as well as by public institutions. This highlights the importance of private companies working in the sector for concrete businesses' aims, therefore the perspective of private companies are taken into account in SecInCoRe. On the other side, the importance of information systems which are publically funded cannot be denied, representing a good solution for implementing and maintaining systems with a high quality of the solution. Unfortunately, these solutions are not so many in terms of number and they have also to face with budget cuts. The systems produced by not-for-profit organisations are a minority but these provide important insights about how information systems can successfully be maintained even without political and economic support.

Certainly the analysis here provided does not pretend to be exhaustive due to the complexity and variety of the field in which the current research is engaged. At the same time it intends to give some insights on the most used approaches, the actors behind the solutions and the scopes when talking about business models.

In conclusion, it should be noted that the identification and definition of business models in this sector could be very difficult due to the many facets and blurred boundaries that information systems have. Furthermore, due to the innovativeness of the sector it is not excluded that business models will change quickly in the future, following further technological development.

6 Access to inventory content

Up to this point, all topics concerning the content of the Inventory have been described. Another important point is the access to these contents, represented in the Knowledge Base. The aim is, to develop a concept for a Semantic Framework, which shows how the content of the Knowledge Base could be accessed easily using the semantics, developed in WP4. This concept should be used as the basis for demonstrators to make the project results from SecInCoRe discussable and visible. After that it could be reused, when organisations plan to prepare their own Common Information Space. The next two sections describe the developed concept and its implementation within SecInCoRe.

6.1 Concept Semantic Framework

The data in the emergency domain within the EU is

- **distributed** among several organisations, persons and storage systems,
- **unstructured** hence stored in several formats and without unified data formats, available in different languages,
- **Available in different languages**, because most organisations are working in their national language and not in English
- **Either public or sensitive or restricted**, depending on the kind of data and the regulations of the nations / organisations.

This causes duplication of effort. Obviously, the problems cannot be solved within a single project, but requires ongoing technical and especially organisational developments in the EU.

6.1.1 Overall

The Semantic Framework matches results of SecInCoRe together to make first steps, solving these issues. Therefore, it uses four main approaches:

- Make the data accessible from one source
- Structure data using semantic approaches
- Try possibilities of automatic translation
- Enable a trusted environment

Having these approaches in mind, the top-level concept shown in Figure 30 was developed. The data in the domain is stored either in databases or in filesystems, spread among all organisations. The data is inserted into the Knowledge Base either connecting the databases directly or uploading the contents of the filesystems. In addition to these data sources, the SecInCoRe databases are connected to the Knowledge Base. Within WP4 different ontologies and semantic approaches were developed, representing broad parts of the emergency domain. These ontologies as well as semantic approaches representing the 'world knowledge' are used to structure the data within the Knowledge Base. Finally, members of the domain could search within the Knowledge Base using the Semantic Search.

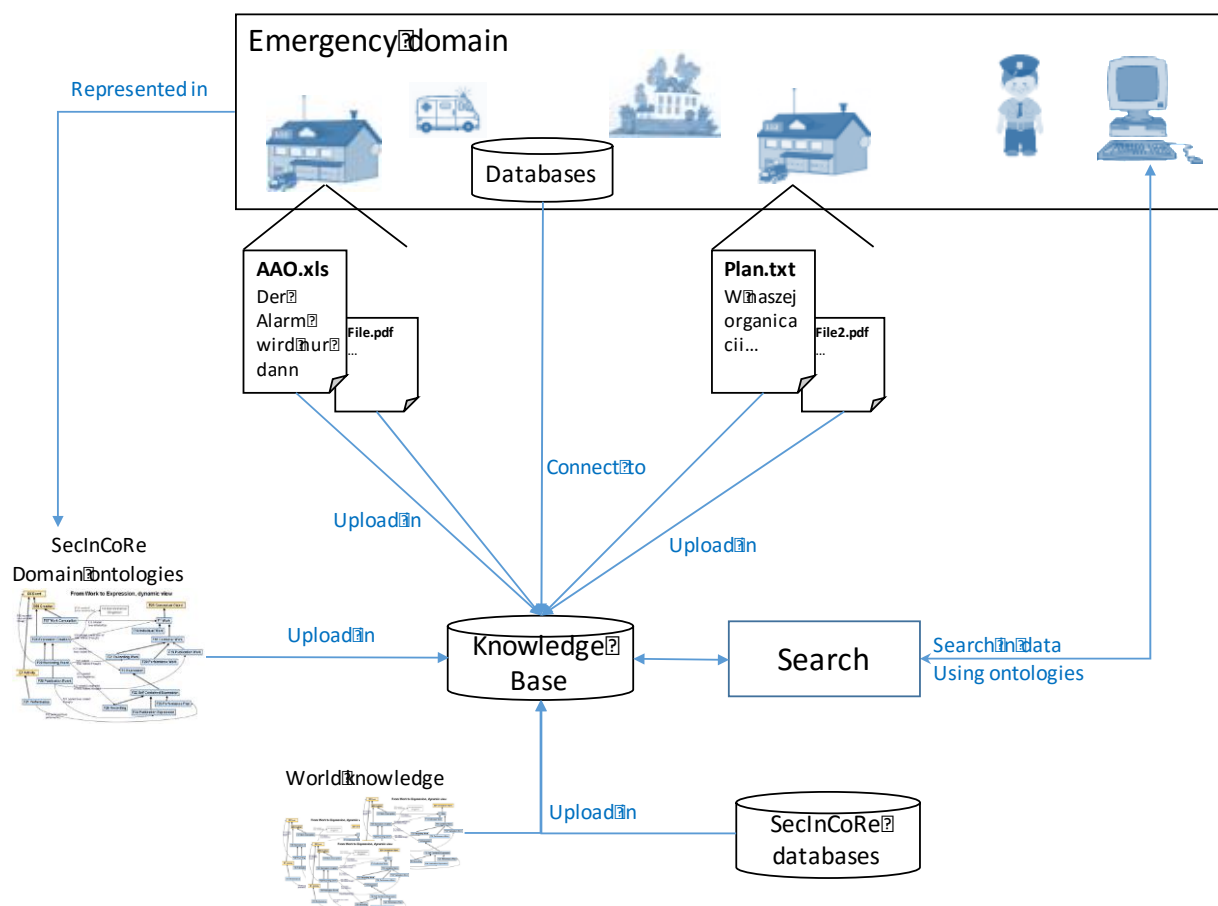


Figure 30: Top Level concept of the Semantic Framework

As explained above, one important approach is the creation of a trusted search/knowledge? environment. Therefore, input from several advisory board members and demonstration case participants was collected, analysed and included in requirements. From this, a concept for how to manage a CIS from the perspective of the Semantic Framework was created. The main question that arose was: Who should host the system, who will be the managing authority? To answer this question, an organisation has to be found, which is **capable** to manage such a system, is able to accept the **responsibility** to run it and is very **trustworthy**. in the eyes of potential participant organisations. Caused by these requirements, a major part of the End-Users agreed that the managing authority has to be on a national level or lower and a governmental institution. As a good first approach the Home Offices of the different nations were identified as managing authorities.

Different national systems could be connected to a bigger European conglomerate managed by a european body i.e. DG Echo or similar, where the details of responsibility and data exchange should be negotiated among the different managing authorities.

There were also End Users who stated, that the managing authority has to be on EU level, but in the last AB-Meeting the structure described here was validated. The resulting organisational structure is shown, using a simple example in Figure 31.

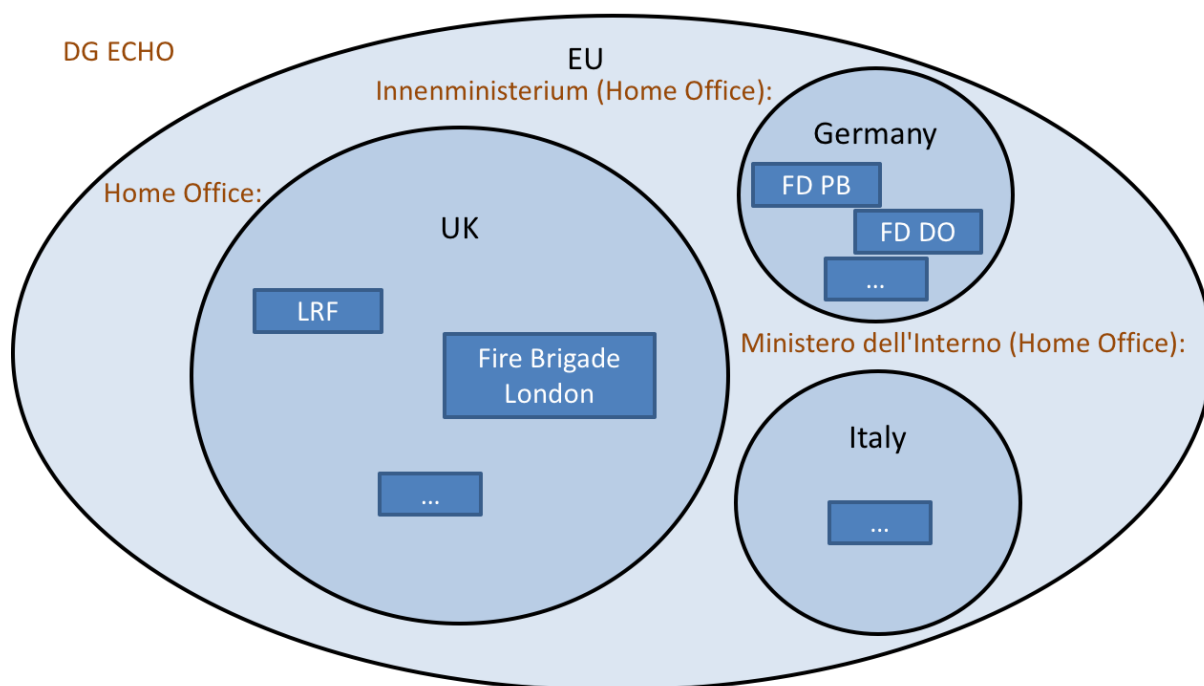


Figure 31: Organisational concept

6.1.2 Data collection

Given that the organisational basis is created, the first question that arise was: How is data inserted into the Knowledge Base? There are two main cases for data inserting: The first one, if data is stored in online accessible databases and the second one, if the data is on the file systems of organisations. After these two, there are several other potential data sources as websites, online storages etc. The Semantic Framework Therefore, enables a broad width of data sources to be integrated. Details about compatible data sources are explained in the implementation section below.

The Semantic Framework envisages two ways to insert data into the Knowledge Base: Either an organisation wants to connect specific data sources to the Semantic Framework or a single user wants to upload a single or a few documents.

In the first case, the organisation has to join the CIS. After that a supervisor defines which data sources should be connected in which way. Either data is uploaded into the Knowledge Base or the data source is linked to the Knowledge Base. Data sources could be file systems as well as single folders on a file system or databases.

Each data source is tagged with a confidentiality level. All documents authors save on these data sources are then treated correspondingly. For the purpose of the Semantic Framework a simplified version of data confidentiality level is used. The details has to be defined corresponding to the specific organisations and to the ELSI guidelines (www.isitethical.eu). The concept of the Semantic Framework offers a flexible adaption. Data sources could be either public within the CIS, sensitive or confidential. Public data is analysed and the document inclusive the meta data is uploaded into the Knowledge Base. If the data source is tagged as sensitive, the documents are analysed and only the metadata is uploaded. The organisation can declare which meta-data should be uploaded for which data source (i.e. topics and title are fine but the summary should

remain private). Confidential data sources are completely ignored by the crawling (Find details in the implementation chapter below).

The last step is the quality assurance: authors and supervisors can optionally review the created meta data and customise or replace it with manual descriptions. Once the documents are inserted, a discussion function for all members of a CIS could enable the exchange among the members and improve the data quality.

The demonstration cases have shown that there are two types of users: On the one hand, there is busy staff who is involved in much daily work. They are only able to use such a system, if it has no or very little influence on their daily workload, by adding tasks to their normal processes. These users will not review the meta data for every document. Therefore, they are happy that the automatic approaches do their job. On the other hand, there are i.e. volunteers or alumni who are very active and write documents, which they happily complement with meta data, or organisations may define specific persons to care in depth with the topic. Therefore, the manual modifying should be an option but the automatic analysis should create the basis. The whole process is shown in the Figure below.

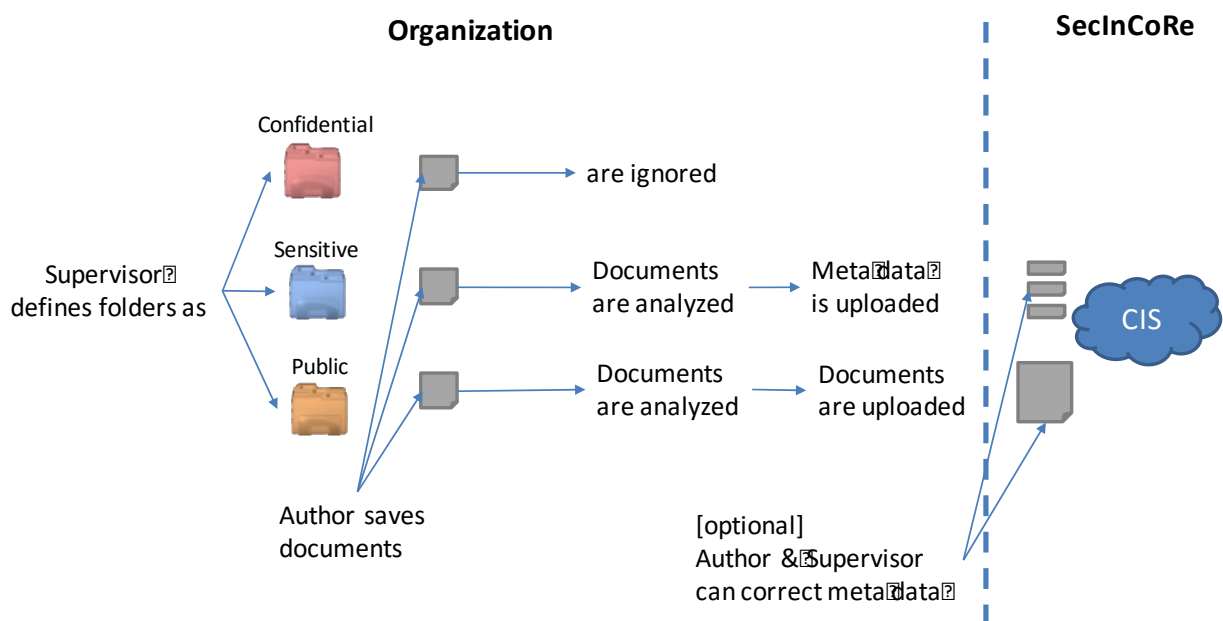


Figure 32: Standard Upload

The second option – the upload of single documents has a similar approach. The organisation of the author has to join the CIS, without mandatorily connect data sources. After that the author uses a web interface to upload his documents. The document is analysed and the author has the chance to modify or replace the automatic results.

6.1.3 Data processing

The analysis process sketched above is divided in several steps. The aim of the processing is to give users within the domain a better overview of documents and their



contents. For that reason, several different approaches are used, utilising both, internal SecInCoRe data and publicly available services.

In Figure 33 the different steps are shown in an example for a document within a pan-European CIS. The document is written in a language other than English. Therefore, users who do not speak or read that language have no idea what this document contains. Therefore, the first step is to translate the document into English. Once that is done, different types of meta data is added. The data source describes the origin organisation of the document. After that the contact details of the author of the document is added. This information should be role specific and not person specific, so that it is not outdated when a person leaves a company. Beneath these data, which could be collected from the LDAP (user role management) servers of the Network Enabled Communication components, there are analysis steps using semantics from Work Package 4 and the world. Two approaches are used to give users a short overview about a document without reading it entirely: topic and summary generation. The topics aim to extract the central subjects of a document. This is done on the one hand using the ontologies created in Work Package 4 to extract domain specific topics and on the other hand public available so called Linked Open Data (LOD) is used. This LOD is public available semantic data about broad parts of the world knowledge. This is needed because of the early stage of similar approaches in the emergency domain. The data is connected semantically and can therefore, be used to analyse documents and finds connections between them. The summary aims to generate a short abstract. It is generated within the project using already built opensource services. To avoid ethical issues, a operative implementation of a CIS has to care about the exact implementation of the underlying algorithms (see www.isitethical.eu).

All this information can be shown aggregated to the end user and gives a better idea what a document is about. The techniques used are not yet in a state where they can provide perfect results. But in a few years, the solutions will be able to give a better translation and description of the documents.

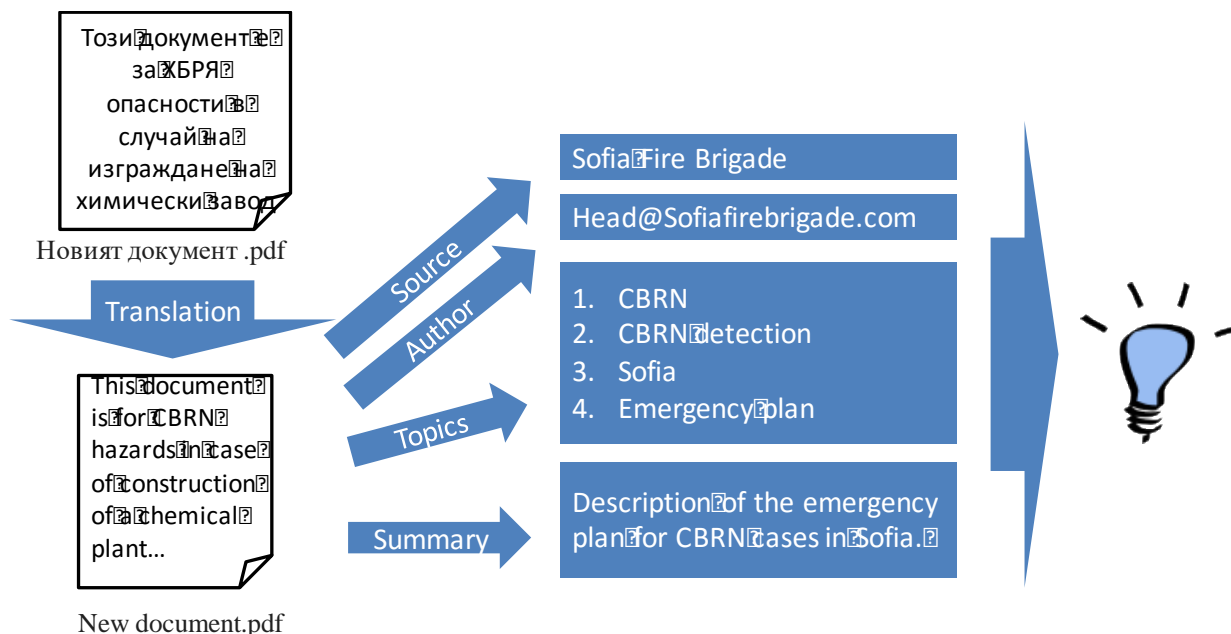


Figure 33: Example of the analysis to understand relevance and content of a document

6.1.4 Quality assurance

One aspect often mentioned by the Advisory Board members and demonstration case participants is the data quality within a Knowledge Base. Data quality in this case is defined as useful data for the members of one CIS. The amount of data contained in a KB is not the main factor for the usefulness, but the kind and quality of the data. Building a KB within a CIS, the balance between openness for contributions and data control has therefore, to fit the specific needs.

SecInCoRe envisages a combination of different approaches to meet this balance. To be in line with all ethical, legal and social issues, the guidelines at www.isitethical.eu is mainly driven from WP2 had to be taken into account. One process implementation is shown in Figure 34 below, nevertheless details of the implementation has to be defined on organisational level, following the ELSI guidelines. The managing authority has the control of the members of a CIS. Therefore, a new organisation which wants to join the CIS (1.) is checked by the managing authority for appropriateness. Once the organisation has joined, it defines one or more supervisors (2.) who are responsible for the actions of the organisations users within the CIS. The supervisor defines then full users and read only users, following organisational rules (3.). The latter can only see documents but not upload documents themselves. The full users can now insert / upload documents into the Knowledge Base (4.). uploaded documents are then processed. After that the full user as well as the supervisor have the optional chance to modify or remove documents or their meta data. After that the data is available within the Knowledge Base for all other member organisations within the CIS. Users from these organisations can now mark documents, they find in the KB as trash (6.). In a last step, a managing authority could either automatically (after x trash-marks) or manually delete marked documents (7.). 'Trash' here means explicitly that rather than 'not fitting for my cause', because results which are not fitting for one user could be very useful to others. That is the same reason why a rating system with stars or similar is technically possible

but not recommended. Data could be of very different value for the very heterogeneous domain users from different organisations, jobs, hierarchy-levels, domain knowledge etc.

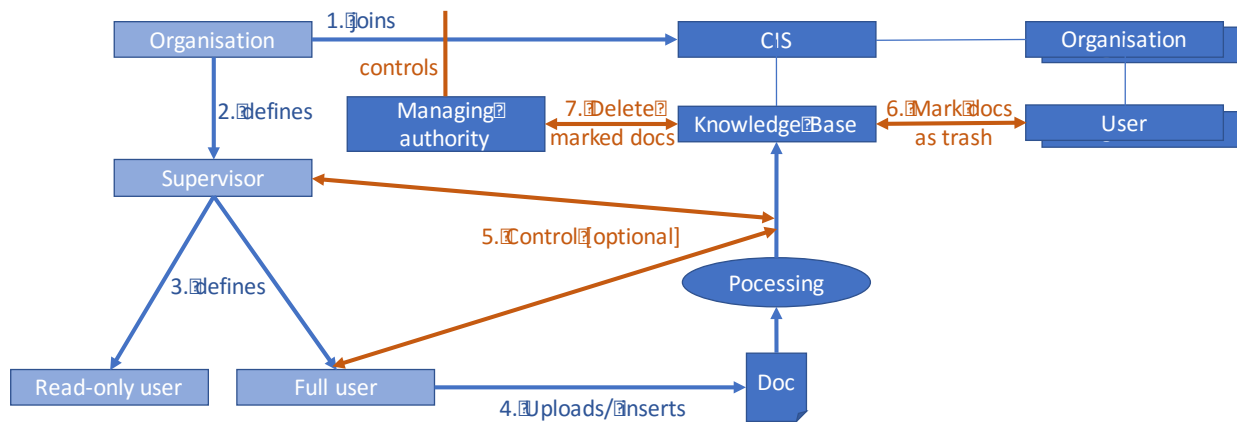
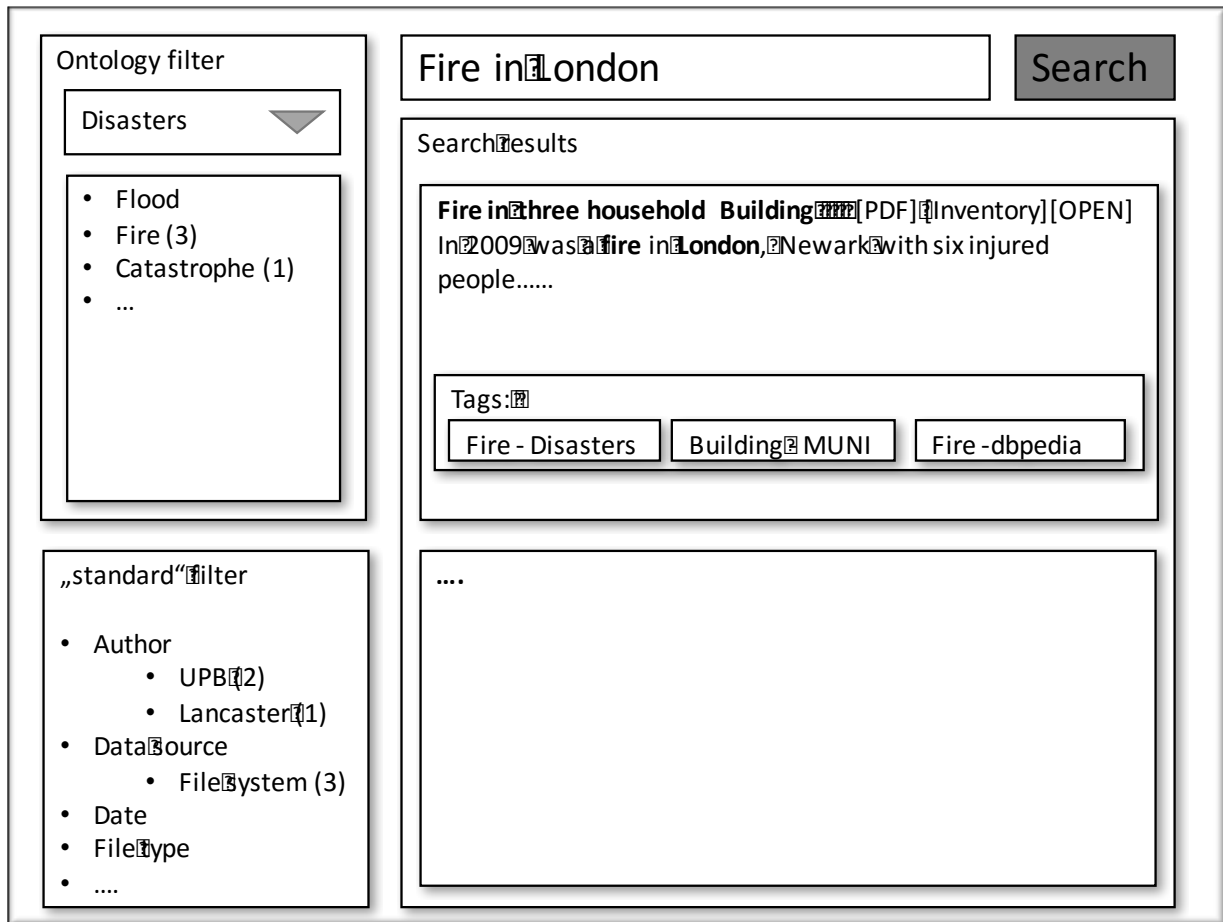


Figure 34: Quality assurance process

6.1.5 Data accessing

After the data is crawled and processed, it is made accessible by the users. The main way to do that is the Semantic Search GUI. It acts like the central user interface to let users search through all Knowledge Base contents, using the processing results to structure and summarise the results. A concept GUI mock-up is shown in the Figure below. The Search is keyword based and gives a list of documents from different data sources as a result. Every result shows its title, document type, data source, associated topics and a summary of its contents. On the left hand, different filter options are available. The results can be filtered by concepts of different ontologies or by standard filters as the author or the data source. As a special view the Graph-View is planned and implemented as proof of concept (described in detail in D4.4). It enables the users to see the documents within their surrounding concepts. Besides the access to the Knowledge Base data with the Semantic Search, there are several ways to access it programmatically. The data layer of the Semantic Framework offers other programs the opportunity to use the data and metadata for their own UI implementation, supporting several flexible API formats.



The mock-up shows a search interface with the following components:

- Search Bar:** Contains the text "Fire in London" and a "Search" button.
- Ontology filter:** A dropdown menu currently showing "Disasters". Below it is a list of categories: "Flood", "Fire (3)", "Catastrophe (1)", and "...".
- „standard“ filter:** A list of filters: "Author" (with sub-items "UPB (2)" and "Lancaster (1)"), "DataSource" (with sub-item "Filesystem (3)"), "Date", "FileType", and "...".
- Search Results:** A box containing a search result snippet: "Fire in three household Building [PDF] [Inventory] [OPEN] In 2009 was a fire in London, Newark with six injured people.....". Below the snippet is a "Tags:" section with three tags: "Fire - Disasters", "Building MUNI", and "Fire - dbpedia".
- Empty Result Box:** A large empty rectangular box below the search results, containing only "...".

Figure 35: Search GUI mock-up

6.2 Implementation of the Semantic Framework

In the section above the high-level concept for the Semantic Framework was described. In this section, the practical implementation is explained.

6.2.1 Research

In the field of semantic systems, there exist a wide variety of systems. Figure 36 gives an overview of different semantic systems and their features regarding data storage, indexing, analysis and search. Additionally, the systems were categorised by their ability to handle external semantic data as ontologies or other RDF data. For the final decision, which system to choose for the task, five systems were tested in detail. Eventually, the evaluation resulted in a decision for the Apache ManifoldCF system in combination with the Open Semantic Framework (OSF). ManifoldCF provides the capabilities to crawl and extract any kind of documents and database data, while the Open Semantic Framework provides the ability to handle storage, indexing and semantic search of the data. Furthermore, custom ontologies can be imported in Open Semantic Framework which are then used as input for semantic analysis tasks like indexing or searching. Additionally, it provides a Web-service API which can be easily accessed from other programs.

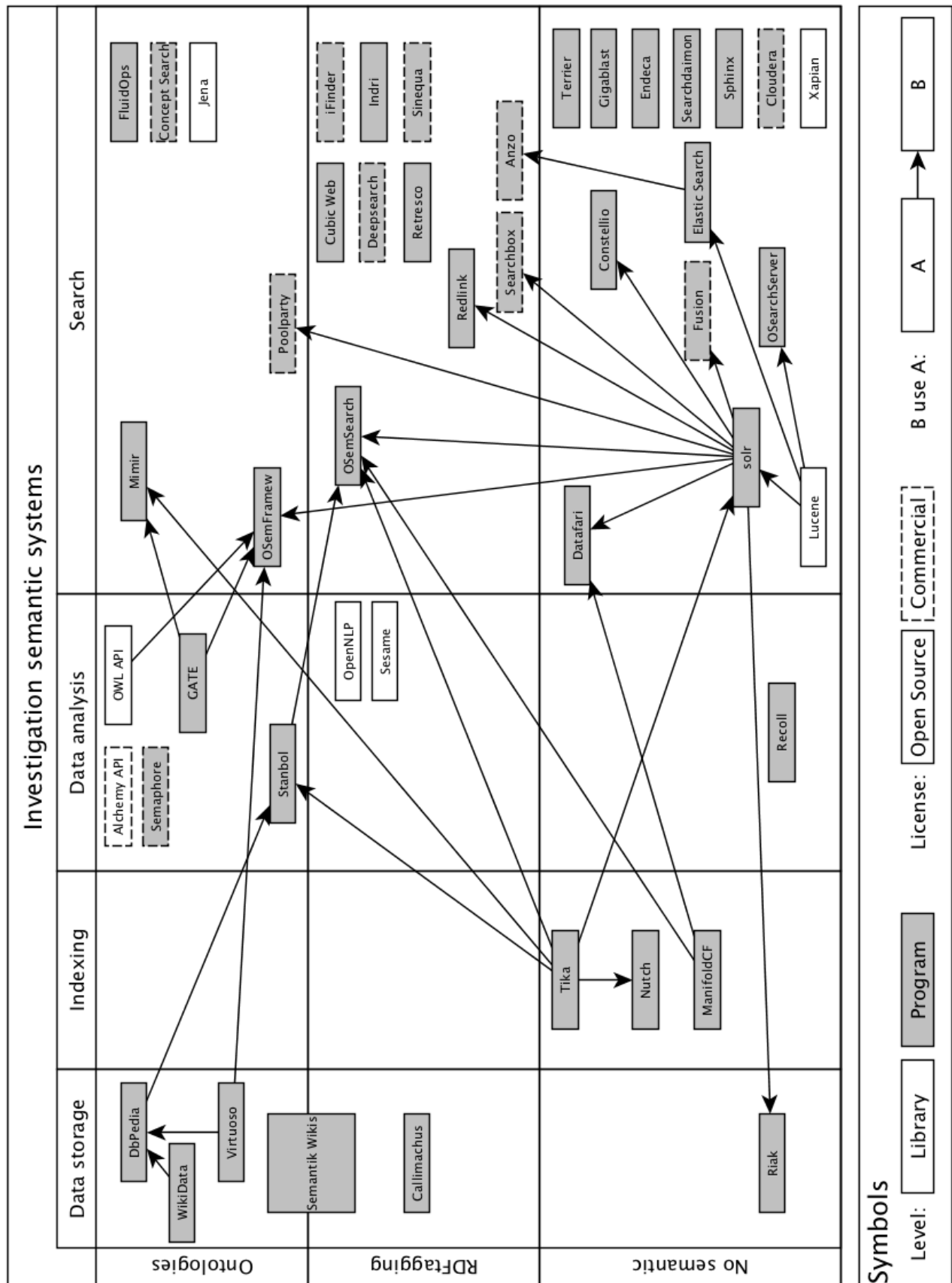


Figure 36: Investigation of semantic systems

6.2.2 Overall Architecture

In this section, the overall architecture of the reference implementation, representing the concepts above, is described. The system consists of several components which communicate through a common interface. The GUI is the frontend component which allows to search for document contents and displays the results and the details of each document (e.g. summary, topics etc.). Additionally, it provides the ability to filter the search results based on the ontology which is used in the OSF system for indexing and searching. In addition, the GUI has a view for the upload of documents from a file system. The OSF system and the GUI are connected via the OSF-PHP API that is an abstraction layer to the underlying OSF Web-services, which contains methods for the creation, update, deletion, read, and search of records (in this case documents and database entries). ManifoldCF is responsible for crawling and processing the documents and database entries and accesses the previous mentioned PHP API to store the processed documents in the Open Semantic Framework.

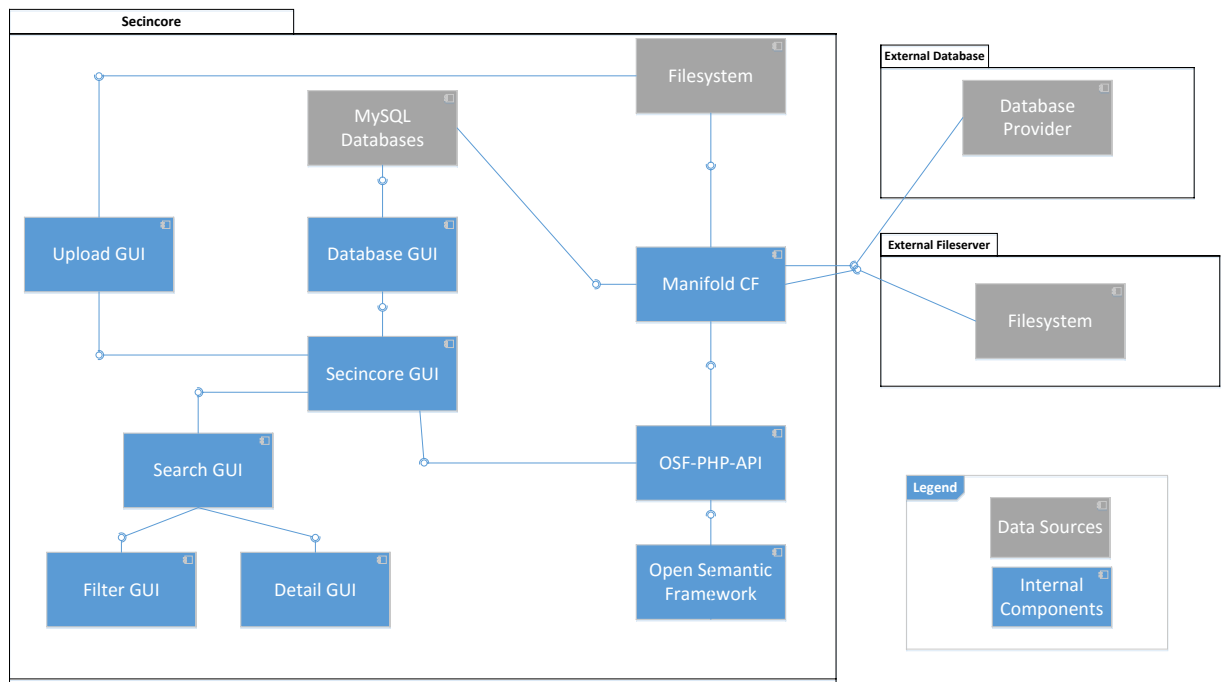


Figure 37: Architecture diagram showing the different core components

6.2.3 Data collection

ManifoldCF provides several inbuilt connectors for different data sources, e.g. filesystem or databases. To demonstrate the concepts, documents from a filesystem source and several MySQL databases are crawled as input for the ManifoldCF system. These connectors are categorised as input or output related connectors. Repository-Connector are used for input and can access data from several different document management systems, databases, websites, among others, while Output-Connector allow the connection to systems where the processed data is stored. All these connectors provide



standard interfaces which can be used to implement a Connector to a custom data source. In this project, a custom Output-Connector was developed to store the processed data in the OSF system. Further custom connectors can easily be integrated into ManifoldCF and activated for processing the data. Apache ManifoldCF supports the following Repository Connectors:

- Alfresco
- Alfresco Web-Scripts
- Amazon S3
- Confluence
- CMIS
- Drop-Box
- Documentum (EMC)
- Email
- FileNet (IBM)
- File System
- Google Drive
- GridFS
- HDFS
- JDBC
- Jira
- Kafka
- LiveLink (OpenText)
- Meridio (Autonomy)
- RSS
- SharePoint (MSFT)
- Slack
- Web
- Windows Shares
- Wiki

Furthermore, these Output-Connectors are supported:

- Amazon CloudSearch
- ElasticSearch
- OpenSearchServer
- SearchBlox
- Solr

A full list and descriptions are available here:

http://manifoldcf.apache.org/release/release-2.6/en_US/included-connectors.html

6.2.4 Data processing

This section describes the process of integrating data from multiple data sources into OSF. Figure 38 shows an overview of the whole process.

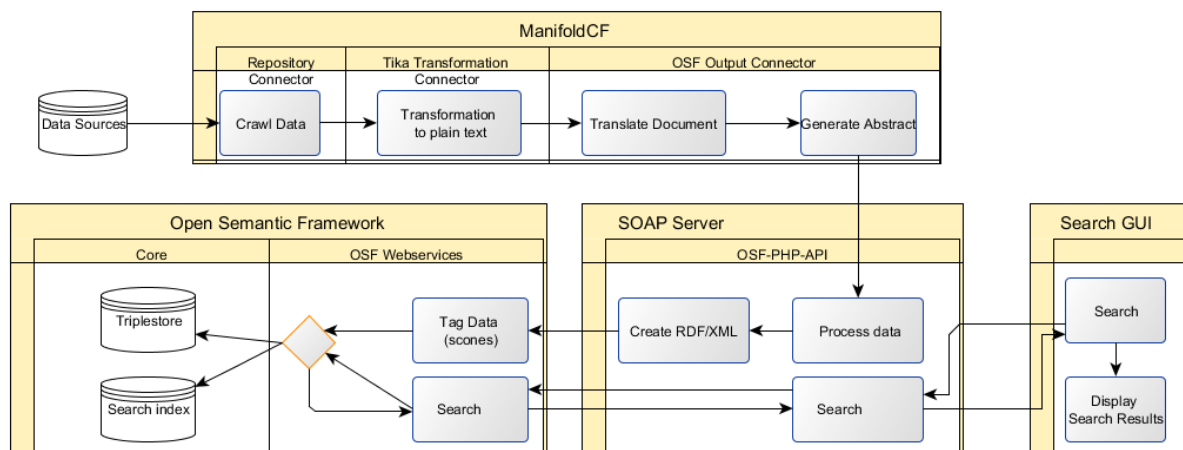


Figure 38: Overview of the crawling and searching process

Data is coming from different distributed data sources. In ManifoldCF, for each type of data source (e.g. file system or database) a so called Repository-Connector is defined that crawls the specified data source in defined time intervals. For every document / database entry, the Tika-Transformation connector is called. In Tika, the various documents / database entries (e.g. text files, PDF, MS-Office) are parsed and cleaned by removing all non-textual parts or transforming them into plain text. Finally, unformatted plain text is produced as output. This text and all available document/repository metadata are then processed by the OSF-Connector. Furthermore, in the OSF-Connector a language analysis using Tika is done, and if the detected language is German, then the document will be automatically translated into English. The translation is done via the Microsoft Translator, which is a cloud-based machine-translation service and could be easily extended for other languages than German. In the next step, the English text (the translated one or the untranslated, if the document text is already in English) is fed into a python script, which uses natural language processing to automatically generate an abstract based on the documents content. Additionally, the OSF-Connector uses the Alchemy API™ service for text analysis to retrieve topics based on the document content. These topics or concepts give the end user a short overview about the document's content. In the background of the AlchemyAPI™ service, several LOD-sources (e.g. DBpedia or Freebase) are used for identifying concepts. Another metadata is the source of the record which is either *filesystem* or, in case of a database entry, the name of the database table. The distinction is necessary for the search GUI to display different details for database entries or documents from the filesystem. Finally, the output, including the plain text, abstract, translated text (if available), untranslated text, and the above mentioned metadata, is sent over the network via the SOAP (Simple Object Access Protocol) protocol to a PHP script which serves as SOAP-Endpoint. The PHP script makes use of the OSF PHP API which allows easy access to the OSF-Web services. Before submitting the received contents into the OSF system, the data is transformed into the RDF/XML format and enriched with concepts from the named entity recognition tagger Scones. Scones is a tagger which searches the text for concepts from the imported ontologies in the OSF system. If a concept is found, the semantic concept from the

ontology is added as a tag to the RDF/XML format. The tagger could be easily replaced with more improved / commercial taggers, establishing a CIS after SecInCoRe project lifetime. Finally, the RDF/XML is inserted as a 'record' into a 'dataset' in the OSF-Framework which makes it searchable.

One record, representing a document or database entry is stored in OSF as shown below:

Record:

recordUri =	The Unique identifier for the document in OSF
documentUri =	The filesystem path of the document on the file server
content =	The extracted document content
fileName =	The filename of the document
contentType =	The mime type of the document
creationDate =	The date when the document was created
datasetURI =	The URI of the dataset where the document is stored
translatedContent =	The document content in English
alchemyTopics =	The topics extracted by the Alchemy API
summary =	The Summary generated from content
author =	The document author
jobType =	The field to distinguish between filesystem and database record

Figure 39: Record of one database entry

Below, the whole process of searching is described. There are two main goals which motivate the usage of the semantic analysis. The first goal is to (automatically) increase the precision as defined in [PKB55] of search queries and the second to provide more and better suitable information for the results of a search query. How these goals are reached is shown in Figure 40.

Initial situation

The initial situation assumes that at least one domain ontology has been created and has been imported in OSF. These ontology sources represent concepts (classes) and instances (instances of the classes) of a specific domain. Once the ontology has been imported, it will be used for tagging when a new document or database entry is crawled and inserted, as described above. Additionally, the ontology is used for search queries, too.

Search by end user

To start a search query, the user opens the search GUI and enters the search term. The Search GUI makes a SOAP request to the PHP-script containing the OSF PHP API. The search query is then forwarded to the OSF-Web service. When multiple search

terms are entered, the OSF-Web service by default performs an AND query, meaning that all terms have to appear in the OSF-record.

Return of search results

The OSF-Web service returns the search results in the JSON format. The JSON is parsed from the Search GUI and all available information is extracted. The search results are then displayed in a list with their title and other information (e.g. abstract, topics, author, and date) attached. Each search result has the option to view and modify details. In case of document detail editing, the edit is limited to the modification of the summary and the topics. Topics can be modified, deleted, or newly added. In the current implementation, database details cannot be modified. If the current selected search result entry is a document, the title is displayed as a clickable hyperlink which opens the document in a new window. The document is retrieved via HTTP from the storage location on the server. In case of a database entry, the detail view opens when the title is clicked. Search results can be filtered by their ontology concepts. The same ontology that is imported in OSF and used for the tagging and searching is also displayed in the GUI as expandable hierarchical tree. This allows easy filtering of the search results by ontology concepts. When a specific ontology concept is selected in the filter view, only search results that this concept or inherited concepts include are displayed.

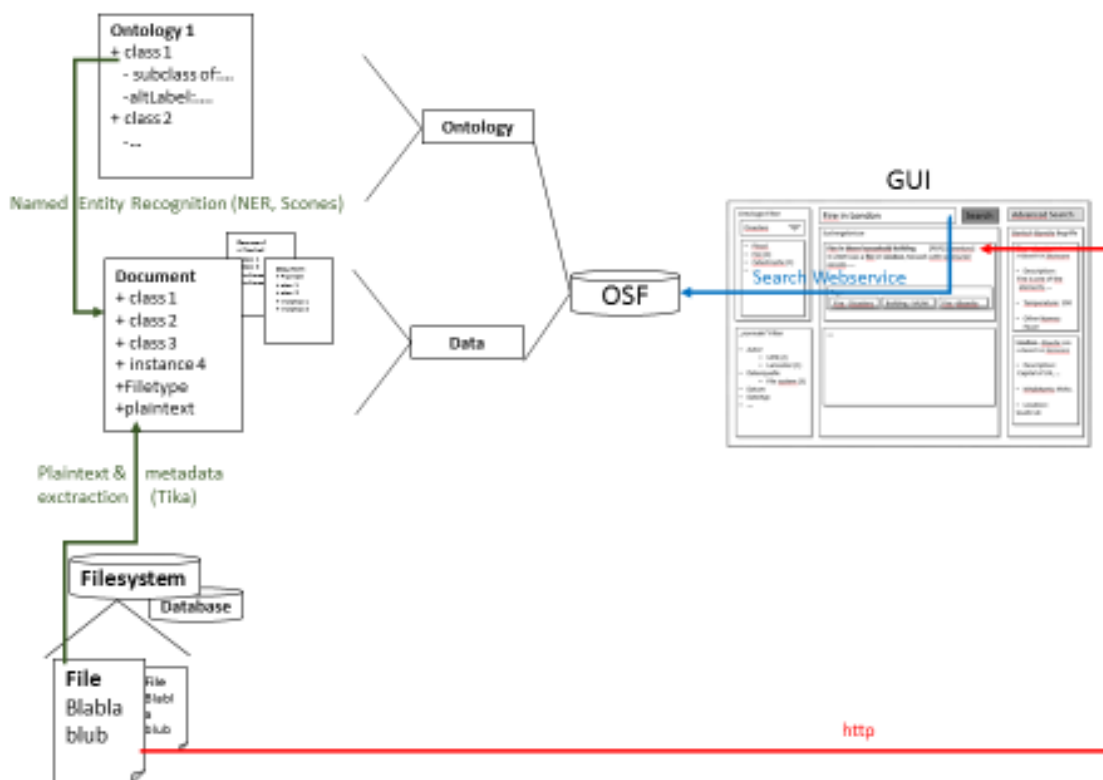


Figure 40: Search results and link to document

6.2.5 Data accessing

This section describes the accessing of the data using the graphical user interface, GUI. The common GUI (Figure 41) consists of several sub components. Main features are the database GUI and the search GUI. All defined databases have the same simple GUI for showing and editing the database contents. By default, the database contents are read-only. However, a click on the *Toogle Editable*-Button enables the edit mode. Boolean values are directly displayed as check-boxes.

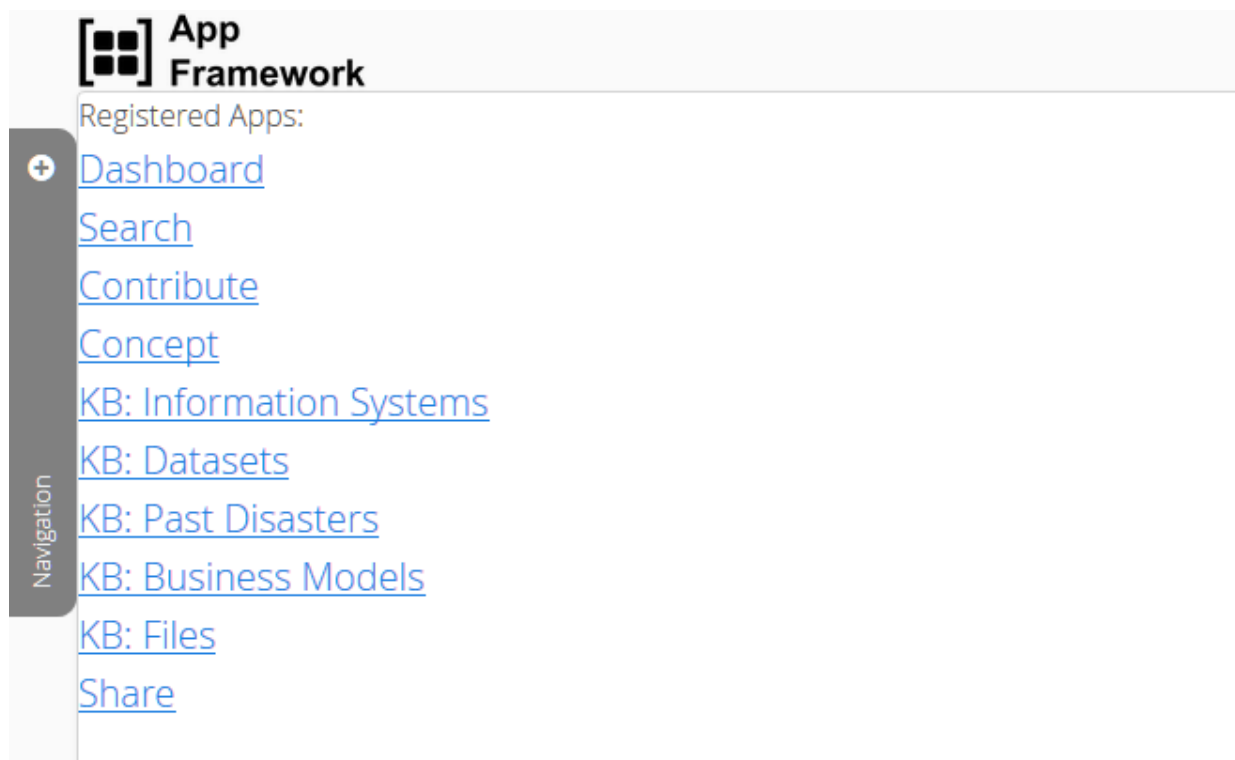


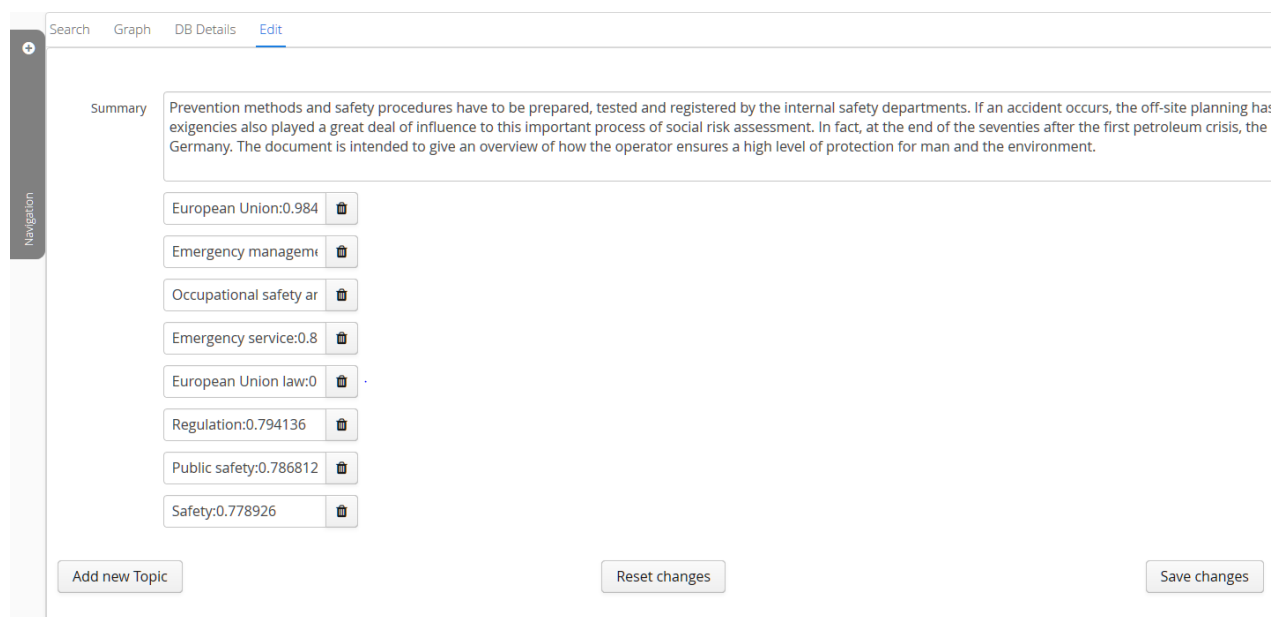
Figure 41: Overview of the SecInCoRe common GUI

The search GUI (Figure 41) is the main component that is responsible for accessing the processed documents and the database data. A new search is started by entering the search term in the search field and hitting the Search button or the Enter-Button on the keyboard. The search results are displayed in a formatted table. In the column *Document* of the table, the shortened document title is shown. On mouse-over, the complete document name is shown. Blue underlined document titles indicate hyperlinks. When a user clicks on the document title, the document is retrieved from the underlying file server and displayed in a new browser tab/window for download. For PDF documents, the document content is displayed directly and can be downloaded, too. As it is sometimes hard to guess the content from the document name, in the column *Topics* next to the document name, the main topics of a document are shown. These topics or keywords aim to give the user a quick insight into the documents content. For example, in Figure 41, seeing the name of the document in the first row, *UK_Cabinet_Office_National*, it is not immediately clear what the document is about. Therefore, a quick look in the second column of that row shows the topics *Risk, Risk*

management, Management, Bank... and the users is now roughly aware of the potential themes the document covers. Furthermore, a click on the black arrow unfolds the detail view, where the document's automatic generated summary is shown. In addition it contains the topics, ordered descending by their relevance, and document metadata, e.g. the author and the creation date of the document.

A Click on the *Edit*-Button opens the Edit-window (Figure 42), where the summary and the topics can be adjusted. As the summary is auto generated using natural language processing, it highly depends on the document's contents and can sometimes generate non understandable sentences. Therefore, it is useful to have the option to edit the summary and to save it for future searches. The same applies to the topics.

The left content pane of the search window is occupied by the ontology-based filter mechanism. The ontology contents are displayed in a hierarchical tree structure and single entities can be expanded or collapsed. The filters are based on a simplified part of the main topics within the ontologies created in WP4. When a concept from the ontology is selected, the displayed search results are narrowed by only showing documents which include the ontology concept in their semantics. When selecting an ontology class, all sub classes in the hierarchical view are also taken into account when displaying the filtered search results.



Search Graph DB Details **Edit**

Navigation

Summary

Prevention methods and safety procedures have to be prepared, tested and registered by the internal safety departments. If an accident occurs, the off-site planning has exigencies also played a great deal of influence to this important process of social risk assessment. In fact, at the end of the seventies after the first petroleum crisis, the Germany. The document is intended to give an overview of how the operator ensures a high level of protection for man and the environment.

European Union:0.984

Emergency managem

Occupational safety ar

Emergency service:0.8

European Union law:0

Regulation:0.794136

Public safety:0.786812

Safety:0.778926

Add new Topic

Reset changes

Save changes

Figure 42: Summary and topic edit mode for document search results



Search Graph DB Details Edit

Filter

- Processes
- InformationSystems
- BusinessModels
- Datasets
 - DatabaseInformation
 - PlanningInformation
 - OperationalInformation
 - ControlInformation
 - KnowledgeInformation
 - OrganizationalInformation
 - ProcessInformation
 - CommandStructure
 - ContactToResponsibles
- Stakeholder
 - PublicSector**
 - LocalAuthorities
 - Politicians
 - HealthBodies
 - Utilities
 - InternationalAgency
 - EmergencyServices
 - NationalAgency
 - Transport
 - PrivateSector
 - CivilSociety

Enter Search term

hazard Search

Details	Document	Topics
▼	UK Cabinet Office National	Risk, Risk management, Management, Bank, Payment system, Hazard, Banking, Causality
▼	GL2016 014 pdf	Public health, Risk, Risk assessment, Risk management, Health care, Health, Emergency management, H
▼	AIHA IMGO Guideline CPC	Cannabis, Carbon dioxide, Tetrahydrocannabinol, Hashish, Hemp, Cannabis, Cannabis sativa, Legality of
▼	Aguirre 2003 Homeland Security	Emergency management, United States Department of Homeland Security, Civil defense, Tropical cyclon
▼	202 pdf	Personal protective equipment, Protection, Respirator, Protective gear, High-visibility clothing, Occupat
▼	6 fy12 hsgp II	Emergency management, National Incident Management System, United States Department of Homel
▲	European industrial emergency planning	European Union, Emergency management, Occupational safety and health, Emergency service, Europea

[European industrial emergency planning](#)

Prevention methods and safety procedures have to be prepared, tested and registered by the internal safety departments. If an accident occurs, the off-site planning has to run, under the leadership of policy makers. Citizen exigencies also played a great deal of influence to this important process of social risk assessment. In fact, at the end of the seventies after the first petroleum crisis, the ecological trend settled in Europe, taking his roots in Germany. The document is intended to give an overview of how the operator ensures a high level of protection for man and the environment.

Topics:

1. Emergency management
2. Occupational safety and health
3. Emergency service
4. European Union law
5. Regulation
6. Public safety
7. Safety

Author: [Torben Sauerland](#)

Source: filesystem

Date: 2007-09-07

[Graph](#)

[Edit](#)

▼	respirator handbook 03 04	Respirator, Permissible exposure limit, Atmosphere, Toxicity, Air pollution, Oxygen, Atmospheric pressure
---	---	---

Figure 43: Search and Filter GUI with search results and details for sample query 'hazard'. The Filter in the left pane allows to refine the ontology elements for filtering.



7 Connections between Work packages

WP3 has relations to various other work packages and research work done in WP3 or related to WP3 is also shown and demonstrated in other WPs and Therefore, part of other deliverables. To demonstrate cross-links and other WP3 related SecInCoRe deliverables the following brief section highlights connections and the flow of research result in the project. The Figure 44 shows up the connections based on the Figure illustrate task dependencies also part of the DOW. Links between other WPs are reduced to set up the focus of the work in WP3.

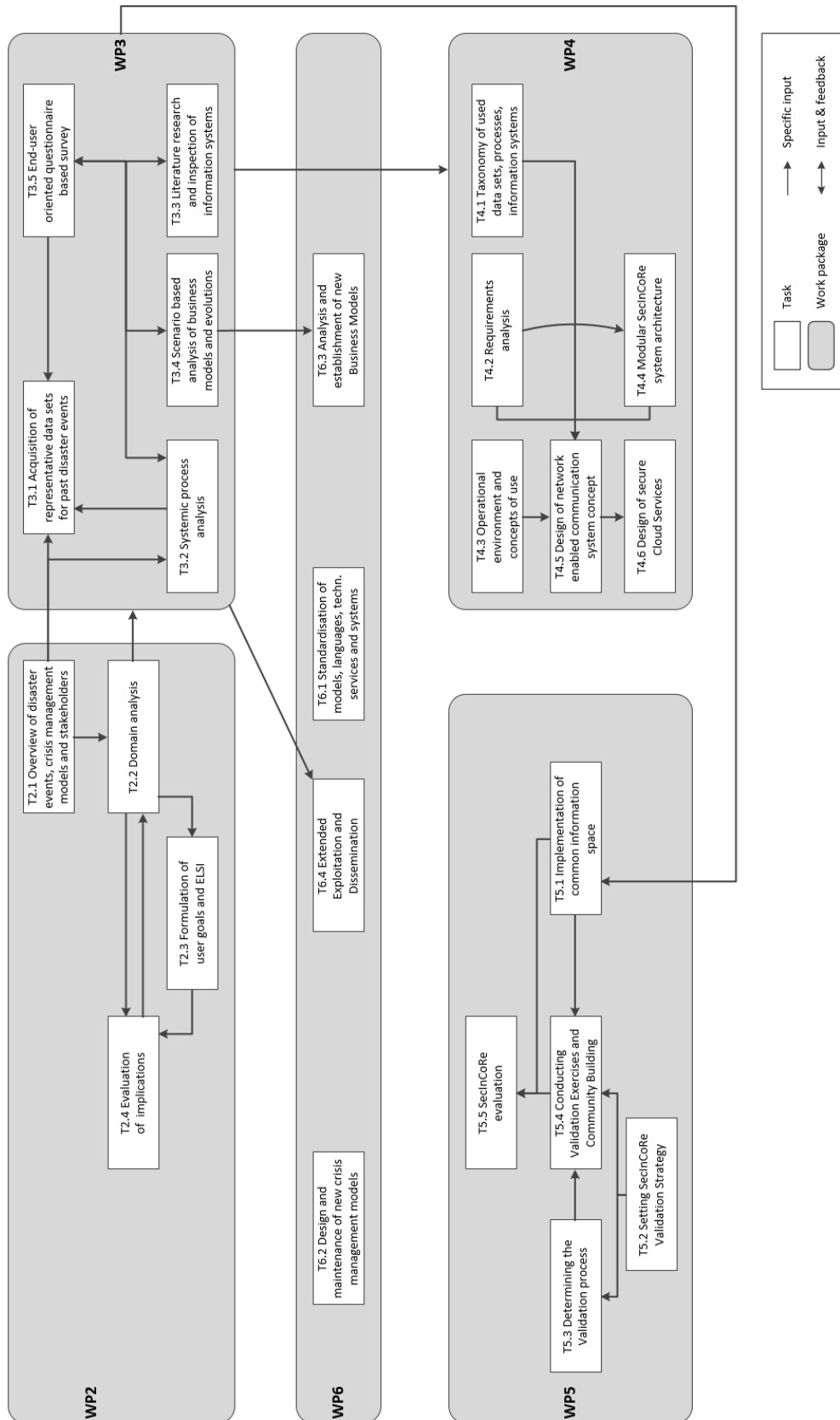


Figure 44: Task dependencies [Figure part of the DOW]

7.1 Relation between WP3 and WP2

Results from WP2 influence the research work done in WP3. Mostly the domain analysis, but also including the different case studies enable WP3 to have a detailed look if necessary in various cases to identify needed or available data sets. Further the analysis of crisis management models was a starting point for the deep analysis of command and control systems in Europe and some non-European countries. Furthermore, the analysis and report on the current databases of representative disaster events mainly in focusing in Europe but not only, have assisted with the definition of the framework and respective configuration of the SecInCoRe structure. The development of ELSI guidance and the various co-designed workshops influence the implementation of semantic services in WP3, i.e. the realisation of a GraphView in relation to transparency for user (mentioned at www.isitethical.eu and D2.7).

7.2 Relations between WP3 and WP4

WP3 provides information in a structured and representative way to support the conduction of a taxonomy and further to derive needed cloud services especially to access the inventory content. These relations are describes exemplary:

7.2.1 Usage of inventory content to derive taxonomy

The usage of inventory content to derive a taxonomy is described in this chapter with the example of combining different command and control systems in Europe.

Overall the development of taxonomies for every single command system serves as visualisation and facilitates an easier comparability. Therefore, it is necessary to analyse the existing documents related to the hierarchical structure. The result should be a structure, where relations in terms of Hyponyms / Hypernyms between the elements become visible.

Hypernyms and Hyponyms:

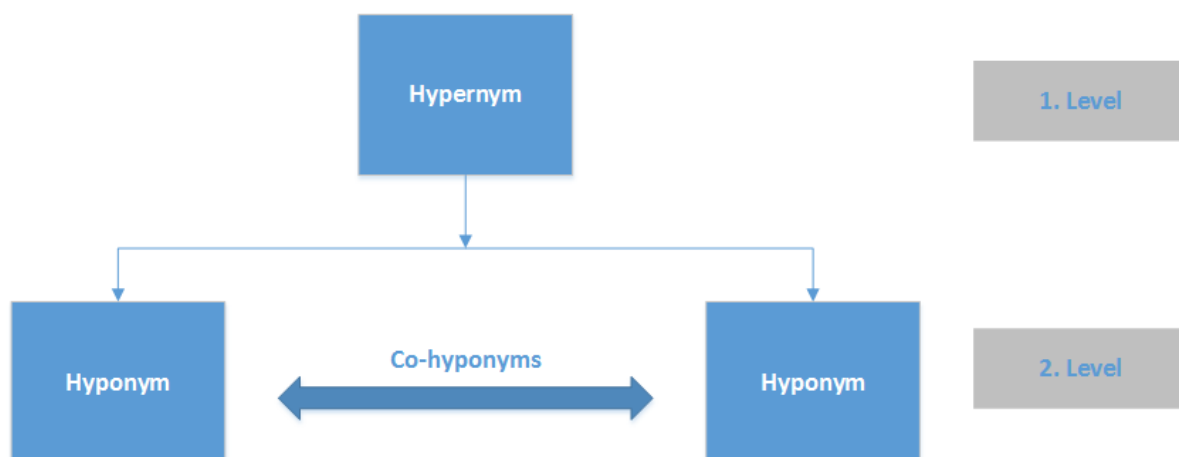


Figure 45: Relationship between Hypernyms and Hyponyms

Hyponymy describes the relationship between more general terms (hypernyms) and more specific instances (hyponyms). The hyponym is an element that shares a type-of

relationship with the corresponding hypernym. The hypernym (superordinate) is in its meaning broader than the hyponym. In general hypernyms consist of one or more hyponyms. The hierarchical structure can be observed from top to the bottom and the degree of specification increases from the higher levels to the lower levels.[www8]

The relationship between the hyponyms of the same hypernym can be defined as co-hyponyms.[www8]

Development of a 'Reference Command System' by definition

The starting point for the development of a Reference Command System is the analysis of the already existing command systems by using their taxonomies. The focus of the analysis is especially on the definitions of single elements. Because of the smallest amount of elements in the ISO 22320, this command system functions as the basis for the comparison. The elements of the ISO 22320 are respectively compared to elements out of the other command systems that seem to have the same purpose and similar positions in the hierarchical structure. Following the definitions of these identified elements are compared and analysed in relation to entire accordance. If the definitions of four elements, each out of a different command system, is almost identical, then a representative element replaces them and is integrated into the taxonomy of the Reference Command System. The hierarchical structure of the combined taxonomy is developed individually and refers to logic relationships of the incorporated elements.

Approach:

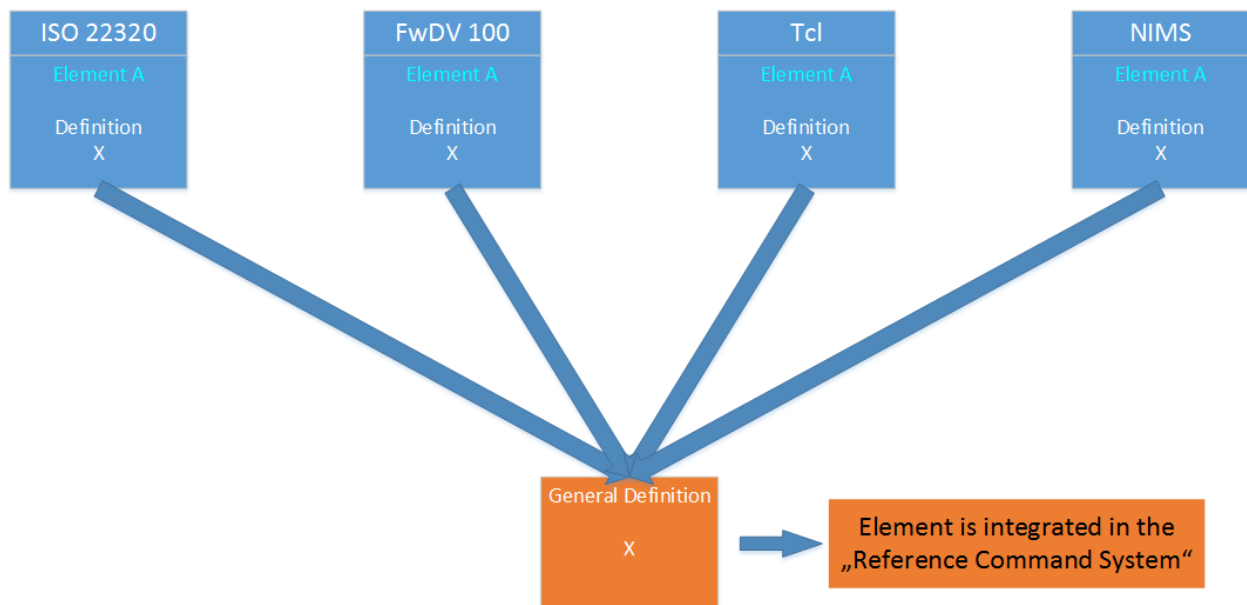


Figure 46: Approach for the Reference Command System by definition

Expansion of the 'Reference Command System'

The analysis of the different command systems relating to single elements is systematically amplified. The purpose is to increase the structure of the Reference Command System and in this context to raise the general significance of the taxonomy. The further analysis does not refer to elements, which are basically identical by definition, but in fact to those elements with similarities in some parts of their definitions or meanings. It must be pointed out that it is not necessary to have entirely the same content between four elements, each out of another command system, because it is sufficient, if there can be identified a partial conformity in the content of these elements. So if these requirements of the analysis are satisfied, then a representative element can be integrated in the Reference Command System. In this case the representative element contains a definition that encompasses only the identified accordance and in addition the complete definition of each element can be archived within the scope of the Template. The integration in the Reference Command System is special for every case and refers, as seen in the analysis before (see 3.1.3), to logic relationships of the elements. The hierarchical structure of the previously developed taxonomy can be changed and has to be adapted according to the new elements.

Approach:

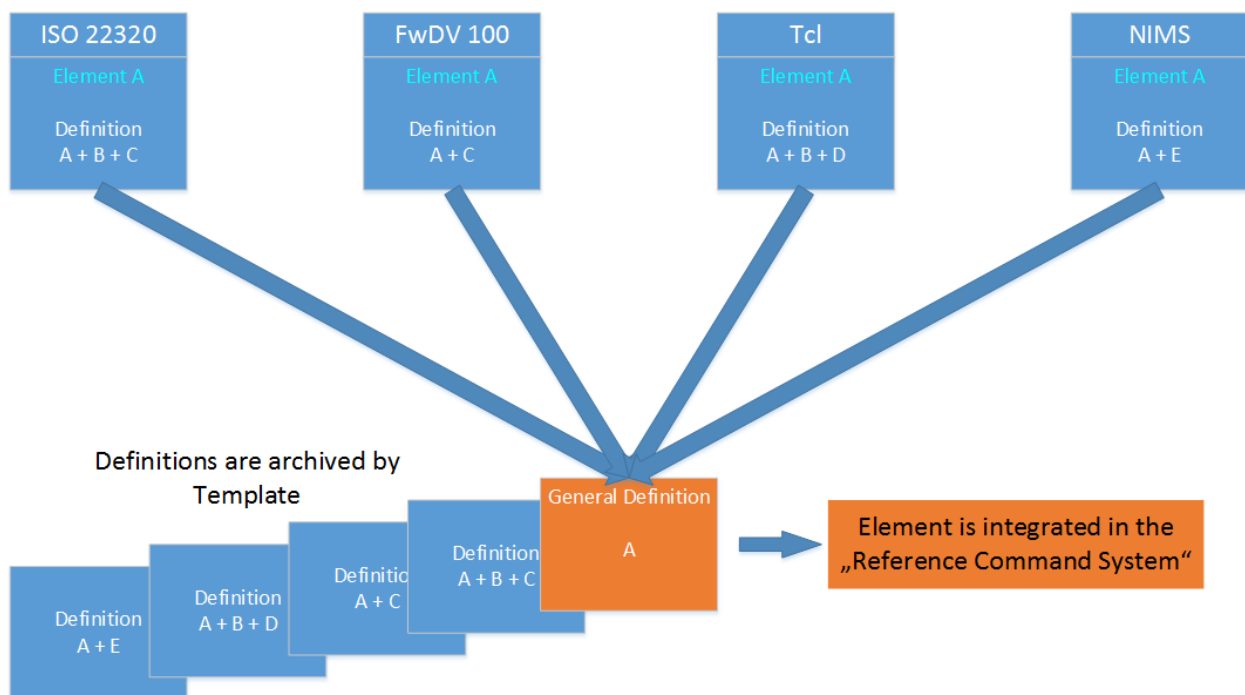


Figure 47: Approach for the Expansion of the Reference Command System

7.2.2 Support defining of semantic cloud services

In D3.3 a detailed analysis of existing information and communication systems has been executed. The results have heavily influenced the work of WP 4 and WP 5 in developing concepts for Semantic Services and Network Enabled Communication as well as their reference implementations.

For that reason the developments of the semantic search functionalities were started. Results are presented in the sections above and also as part of the cloud service infrastructure in D4.3.

Barriers mentioned in D3.3, like non-existent cross-border communication, have been directly addressed in the ongoing work of SecInCoRe. The RescueRoam concept as introduced in D4.3 provides an easy-to-use access to the CEIS for all participating organisations. The analysis of approaches to facilitate the usage of heterogeneous communication technologies like 4G, WiFi, TETRA etc. supports ad-hoc communication on-site and off-site emergency situations. Figure 48 depicts the generic communication architecture of SecInCoRe incl. a secure and trusted access to the information system.

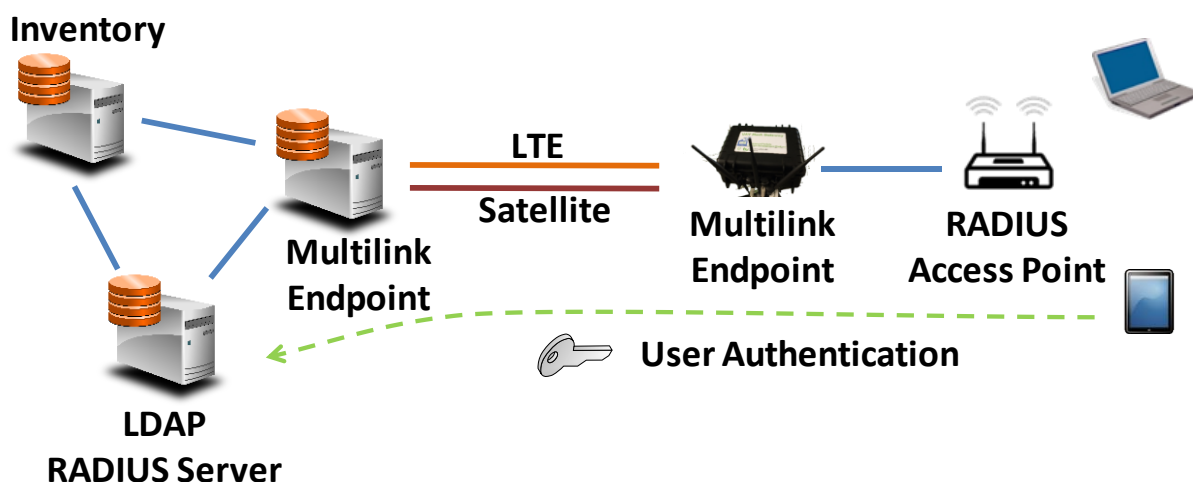


Figure 48 Generic communication architecture incl. RescueRoam (see D4.3, D4.4 for details)

7.3 Relations between WP3 and WP5

To enable significant results related to defined demonstration cases data, documents and information have to be present in the case. This work was also driven by WP3, to ensure a functional process during the demonstration case. Knowledge base and semantic search were also part of demonstration cases to get validation insight.

7.4 Relations between WP3 and WP6

A major amount of results from WP3 are included in the exploitation process and some parts are also input regarding standardisation activities (See D6.4). For example work done by Prof. Dr.-Ing. Rainer Koch in relation to the ISO 22320 was influenced by research results from the analysis of command and control systems.

8 Verification and Validation of Inventory, Knowledge Base and Search

The following table describes the High Level Requirements (HLR) considering the process and development of the inventory, the Knowledge Base and the search functions to access the Knowledge Base. Details are described in D4.1.

To define in detail steps and goals for the development of the inventory related elements, a transformation into smarter requirements is necessary. A HLR is assigned to one or more components and outcomes of the SecInCoRe project. Therefore, the fulfilment of the requirement can only be ensured by a specification of all low level requirements (R1,...,R3 in the following Figure) for each component. The approach is shown in the Figure below.

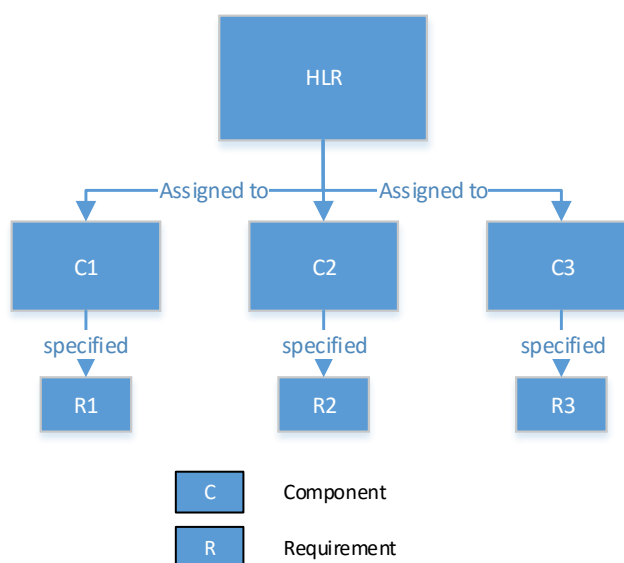


Figure 49: Connections between HLR and the different components

The results of the verification and validation are shown in the tables below.

8.1 Inventory

Number of requirement	Description of requirement	Transformation	Verification and Validation result
SICR-149	Information aggregation should be based on reliable sources of information	The inventory will base information aggregation on reliable sources	Different data sources were analysed and aggregated to higher information. For each task dedicated research approaches are designed and build the basis for a valid research. Literature inspection enable the use of trusted literature, further data was gathered from end-user and market study.



SICR-139	ELSI in the structuring and representing of data	The inventory will respect ELSI in the structuring and representing of data	There was a close relationship between research results of WP2 and WP3. Further the design of the search was often part of co-design workshops with several end-user. For this reason ELSI was part of the structuring and representing of data, but see more in the description of the search functions.
SICR-128	Support users in making the most of data	The inventory will support	Various representations of search results and Therefore, of presentation of data was analysed and partially implemented. I.e. the GraphView functionality come up with the idea to present documents in their context in an ontology.
SICR-127	Support graceful augmentation	The inventory will provide an analysis of existing information management processes without a force for first responder organisations to change them	In the analysis of existing processes and command and control processes of Europe different practices were identified. The results are described in D3.3 and D3.4 and published in the search function and the knowledge base. In this order alignments between the practices were shown but first responder organisations were not examined to take practices over, but are aware of differences that support collaboration.
SICR-122	Support social and organisational practices of interoperability	The inventory will collect and analyse social and organisational practices of interoperability.	The analysis of information management processes and command and control system in various European countries are part of the inventory.
SICR-119	Support non-discriminatory practices	The inventory will not contain discriminatory content.	The inventory is written by researcher and based on valid research studies and literature inspection. The inventory is built on reliable sources.
SICR-117	Support diversity across nations, agencies, users.	The inventory will contain processes, information systems and data sets from several European countries	The deliverables D3.2, D3.3 and D3.4 demonstrate research results from different nations and Therefore, show up the diversity in Europe. The WP 3 research approach enables user to be aware of differences without the force to change own practices. I.e. the



			refugee crisis were analysed from a high-level perspective in the past disaster studies, and then including a detailed look from a Greek and German perspective.
SICR-109	The number of persons performing data aggregation should be limited	The inventory will limit the number of persons dealing with data aggregation	The inventory is a result of researcher within the SecInCoRe project. By the nature of the inventory the number of persons dealing with data aggregation is limited. End users were invited to co-design workshops to dedicated topics and results were analysed and reflected before integration in the inventory.
SICR-108	Support compliance with the freedom of information act	The inventory will be published to the public	Results of the analysis of WP3 will be published in various deliverables. The knowledge base contains results of the inventory and is open to the public during the project phase, please see requirements of the knowledge base and the description in chapter 6. In order to be aligned with the principle of the managing authority of a CIS the knowledge base of a dedicated CIS will not be open to the public to support first responders and Police authorities in their daily work and keep the quality of the databases in a high-level. The special requirements are covered within the ELSI guidelines.
SICR-104	Support practices of sense-making and information management	The inventory will be presented in an understandable way	All deliverables of WP3 are public and written to present other researcher, first responder and the public results of the analysis of data sets, processes, information systems and business models.
SICR-103	Support users in respecting human rights	The inventory will not infringe human rights	The inventory deals also with hot topics like the refugee crisis and aims to present information management processes and used data in a neutral way. The

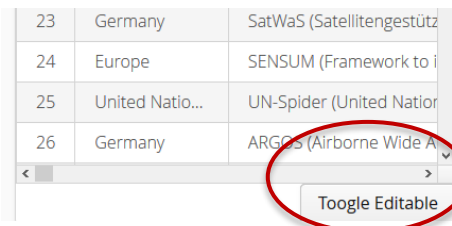


			inventory does not infringe any human rights.
SICR-73	Ensure the quality and correctness of entries	The inventory will ensure the correctness of data	The inventory is based on reliable sources and aims for a high quality
SICR-55	Clarity of Data	The inventory will ensure the clarity of data	The inventory is based on reliable sources and aims for a high quality
SICR-53	Ensure completeness of data	The inventory will ensure the completeness of data	The inventory is based on reliable sources and aims for a high quality. A completeness of all data in Europe is not possible but significant amount of data was gathered.
SICR-52	Ensure correctness of Data	The inventory will ensure correctness of data	The inventory is based on reliable sources and aims for a high quality.
SICR-48	Kind of information provided	The inventory provide different kind of information	The inventory provide information dealing with data sets, information systems, processes and business models.
SICR-47	Long stand-alone operation for any portable device	Reject – the inventory is a non-technical analysis and don't aim support long-standalone operation	
SICR-41	SecInCoRe should be energy-efficient	Reject - the inventory is a non-technical analysis and doesn't aim to be energy-efficient	
SICR-40	SecInCoRe should not incur additional expenses	Reject - the inventory is a non-technical analysis and doesn't aim to be economically affordable	
SICR-38	SecInCoRe should be economically affordable	Reject - the inventory is a non-technical analysis and doesn't aim to be economically affordable	
SICR-36	Real-time use	Reject – during the project the focus to preparation and preparedness to disasters change	



SICR-35	Based on already existing technologies and processes	The inventory will based on existing technology and processes	The inventory uses existing approaches and systems. All implementations, structuring approaches and data is based on existing Open Source or commercial systems.
SICR-31	SecInCoRe should be resource efficient	Reject - the inventory is a non-technical analysis and doesn't aim to be resource efficient	

8.2 Knowledge Base

Number of requirement	Description of requirement	Transformation	Verification and Validation result
SICR-189	Produce an improved awareness of the infrastructures within/causing/supporting disasters	Reject – the focus of the project is based on the support of preparation and preparedness to disasters	
SICR-153	Create flexibility so that the system can incorporate new sources of data	The Knowledge Base will enable the incorporation of new sources of data	Each data base included in the knowledge base allows the integration of new sources. 
SICR-98	SecInCoRe users need an improved awareness of past disasters	The Knowledge Base will provide a dedicated data base containing relevant content of selected past disaster	The knowledge base include a dedicated past disaster data base. A detailed definition of the database is documented in D2.5.



			<div> <div>date_start</div>06.04.2009 <div>date_end</div>08.04.2009 <div>coordinate_reference</div>42° 20' 56" N, 13° 23' 53" E 42.348889°, 13.398056° <div>area_complete</div>Null <div>bibliography</div> <p>Braun, T. (2010). 'Non è il terremoto che uccide'. In F. Banti, A. Girometti, & F. Sancosiani (Eds.), On Caporale, G. (2009). 'Così il sindaco chiese aiuto prima del sisma'. La Repubblica, 18th April. Available at: Centro Regionale di Studi e Ricerche Economiche Sociali (CRESA), (2009). Economic consequences of Daphne, E. et al. (2010). WPC: Integration and Connection of Vulnerabilities Del. 2.1.3 Relation to ENSURE Project. (2011) WP3. Vulnerability in time and space. Del. 3.2. Analysis of vulnerability factors. Imario, M. and Firenze, S. (2009). 'Barbari e il dossier dimenticato: erano tutti i palazzi crollati'. L'Espresso, (2009). Verbale della commissione Grandi Rischii (Aquila, 31 marzo 2009). Available at: Munich RE. (2009). Topics Geo Catastrophes natural 2009 Analysis, valoraciones, Posiciones. Presidenza del Consiglio dei Ministri (PCM). (2009). Relazione della Commissione Ambiente del 10 Rapporto, B. (2009). Censimento di vulnerabilità degli edifici pubblici, strategici e speciali delle regioni.</p> <p>Scalzo, A. (2010). 'Ore 3:32: il sisma colpisce nella notte: descrizione catena delle informazioni dal s' http://www2.regione.piemonte.it/protezione civile/index.php/progetti-europei/interreg-risknat/cor</p> <div>description</div> <p>In the night of 6 April 2009, a 27 seconds earthquake occurred in Abruzzo region, in the central part of the region (e.g. the center of L'Aquila which also had the highest percentage of dead people), 11 buildings. The relevance of the event concerns also the fact that the earthquake has strongly hit activities.</p> <div>image</div> <p>http://www.secincore.eu/wp-content/uploads/2015/06/2.3.12-L'Aquila-Earthquake_Italy_2009.jpg</p> </div>
SICR-85	System should be able to estimate the evolution of the disaster	The Knowledge Base will have a database including the evolution of a disaster	<p>The past disaster database as one part of the knowledge base describes the impact of past incidents as shown in the following Figure. Moreover a timeline of the incident is presented.</p> <div> <div>damage_Material</div> <p>The event not only destroyed the oil depot, but it also destroyed various commercial and residential buildings near to the site, as well as affected buildings in up to a 5 mile (8 km) radius around the site (e.g. with broken windows, damaged walls, ceilings, etc.). The explosion and fire resulted in</p> <div>impact_SocialHuman</div> <p>While over 40 people were injured by the explosion and subsequent fire, there were no fatalities. That being said, approximately 2000 people needed to be evacuated from their homes, and parts of the M1, M10, and M25 motorways were closed resulting in considerable disruptions. Some</p> <div>impact_Economic</div> <p>According to the Buncefield Major Incident Investigation Board's Final Report (BIIIB 2008): "The estimate of total quantifiable costs arising from the Buncefield incident comes close to £1 billion." (p. 24). The sectors included in the costs are: site operators (compensation claims) (£625m), aviation (£245m), competent authority and Government response (£15m), emergency response (£7), and environmental impact (£2) for a total of</p> <div>preparedness</div> <p>The Buncefield Major Incident Investigation Board's (BIIIB 2008) Final Report argues that the event was caused by the failure of an on-site alarm to stop tanks from overfilling. While an on-site emergency plan was in place (i.e. developed by the Oil Depot), the Report argues that it had not taken into consideration the potentiality for such a major incident. It goes on to argue that: "The impressive emergency response to Buncefield effectively relied on initiative and good working relations of the responders in dealing with an incident that had been unforeseen and therefore not planned for." (BIIIB 2008: 51, emphasis added). This reliance on 'initiative and good working relations' between</p> </div>
SICR-73	Ensure the quality and correctness of entries	The Knowledge Base will support procedures to ensure quality and correctness of data	The Knowledge Base contains of several inventory related data bases. In a first step data is gathered in a defined research approach. The data bases are open in the consortium to change inserted content. Further non-relevant or misinterpreted able content was identified during demonstration cases. The search functionality provide further options to support quality of data.
SICR-33	Clear usability	Reject – the question of usability is not needed for the data bases of the knowledge base and not main theme of the project	



SICR-153	Create flexibility so that the system can incorporate new sources of data	The Knowledge Base will support to include new sources of data	The Knowledge Base support the inclusion of new data sets in the respective data bases.
SICR-126	Support people in keeping the inventory and/or the CIS relevant	The Knowledge Base will support procedures to keep the inventory content up-to-date	The Knowledge Base allow to delete old content or include new content.
SICR-116	Support equal access	The Knowledge Base will not exclude people by design	Access restriction depends on the design of the CIS and the respective managing authority. The knowledge base itself will not restrict the access and during the project time it is open to the consortium but also to the public. In order to be in line with restriction to sensitive data a restriction to access content of the knowledge base in foreseen.

8.3 Search

Number of requirement	Description of requirement	Transformation	Verification and Validation result
SICR-125	Support people in cooperating without infringing on the sovereignty of other organisations	The search should support cooperation between organisations. Every organisation should decide free and transparent, which data is shared and which is confidential.	The organisations have always the full control of their data. They can specifically decide which data is shared and which not. After that the managing authority is a national governmental organisation which is trusted by the participating organisations.
SICR-124	Support people in recognising CIS as a common space	The search should be a function of a common information space enabling	The search enable access to different data sources without the need for user to switch between different filesystems, etc. Further



		the connection to different data sources.	there is conceptually and partially technical developed the integration of the search and other components available, so that the CIS the concept of a common space from a technical perspective. Further the development was supported by WP2 to ensure the consideration of possible ELSI.
SICR-119	Support non-discriminatory practices	The search should not contain functions or data analytics which discriminate people.	The search differs in no way between people of different race or religion etc..
SICR-118	Strive for simplicity in design	The search should not focus on irrelevant content or distract the user from the data .	The search and it's UI focusses on the display of the data and the structuring elements. No distracting of users is obvious.
SICR-117	Support diversity across nations, agencies, users.	The search should enable access to the Knowledge Base from all over the EU.	The Search is a web based tool and Therefore, available from everywhere. The language is English as the most spoken language. A translation after the project in other languages is easily possible.
SICR-116	Support equal access	The Search will not exclude people by design	Access restriction depends on the design of the CIS and the respective managing authority. The search itself will not restrict the access and during the project time access to the knowledge base via the search is open to the consortium but also to the public. In order to be in line with restriction to sensitive data, a restriction to access content of the knowledge base in conceptually foreseen in the search function.
SICR-115	Support accessibility		The search doesn't prevent anyone to use it. Special implementations are not used, because of the demonstrator status of the implementations. Special aspects of the demonstrators could not be used by some disabled people because of their complex visual elements.



SICR-114	Support inclusiveness through search		The search doesn't hinder anyone to use it. Special implementations are not used, because of the demonstrator status of the implementations.
SICR-113	Support informational self-determination	The search should enable users to edit and remove their own data.	The organisations are able to remove data sources from the search and authors could edit metadata of the search entries.
SICR-112	Alert users to danger of unlawful re-identification	The search should inform the users, if he could be identified with a document.	All data uploaded in the Knowledge Base is tagged with the authoring organisation. Therefore, every user has the clear information, that his authorship is public within a CIS.
SICR-111	Support practices of managing privacy or Design FOR privacy	The search should not collect more personal data than necessary.	The search collects only the name of the author and the organisation which is responsible for a document. No other personal data is processed. All data is stored safe and encrypted in concept. In demonstrator no personal data is gathered..
SICR-110	Support obtaining informed consent or exception		An operational implementation of the search concept will care with informed consent, as the search is part of the Collaboration platform, which can cover that aspect. For the use cases within SecInCoRe demonstration cases, this aspect is done organisational instead of in the implementation.
SICR-109	The number of persons performing data aggregation should be limited	The search should not allow all people to aggregate data	The search enable a semantic access to different document or data sources. The aggregation is not possible without illegal methods.
SICR-108	Support compliance with the freedom of information act	Reject – access to the knowledge base via the search is possible. But depending on the design and the managing authority of a CIS not all information could be provided to everybody.	

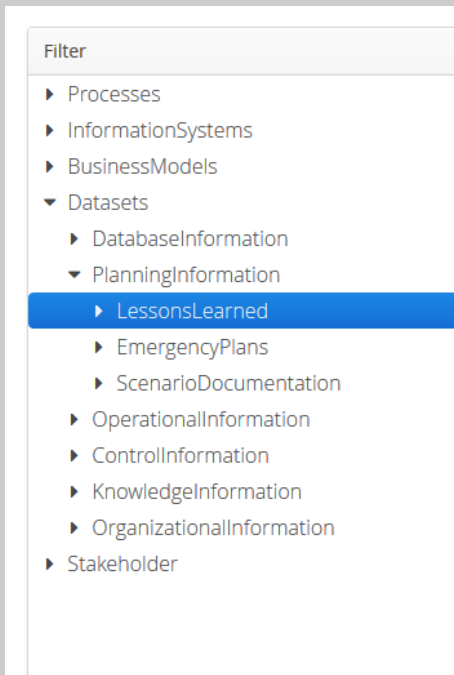


SICR-106	Support users in complying with privacy by design and privacy by default principles	The search should allow people to restrict access to personal or data source related information	Conceptually and partially implemented are mechanism to leave the decision about access restriction to the organisation of the document.
SICR-104	Support practices of sense-making and information management	The search should be based on practices of sense-making & information management.	The search uses several practices of information management and it supports the sense-making of data as much as possible, using several semantic and manual tagging and analysis functions.
SICR-103	Support users in respecting human rights	The search should not infringe human ights.	The search doesn't infringe human rights.
SICR-102	Support users in balancing security (as in resilience to disasters) against the right to privacy.	The search should allow user to restrict access to documents.	When contributing information to the search there is the ability to restrict data. Further guidance are developed in WP2 to cover issues on access restrictions.
SICR-92	Enable different level of detail of information	The search should enable the view on the data on different detail levels.	The search has an overview (The result list) as well as a detail (result view) view.
SICR-24	Support for classification of information	The search should make the classification of the content visible, which was developed in WP4 and the Inventory. After that the search should enable users to modify tags, which are automatically generated.	The search visualises the the classification as filters as well as a graph view. After that, it enables users to modify tags of documents and thus actively engage with how their material is classified.
SICR-20	Classification of information	The search should make the classification of the content visible, which was developed in WP4 and the Inventory. After that the search should enable users to modify tags, which are automatically generated.	The search visualises the classification as filters as well as a graph view. After that it enables users to modify tags of documents and thus actively engage with how their material is classified.

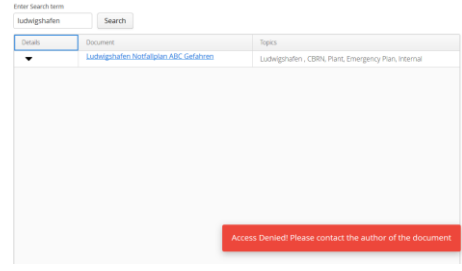
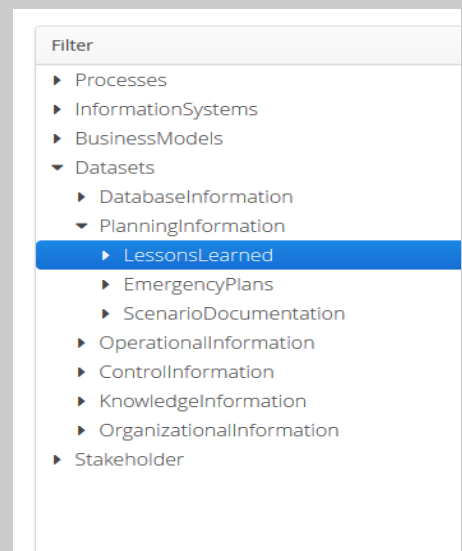


SICR-7	Search History	The search should store a search history.	The search stores the history of searches in the backend but not in the frontend, because there was no user-based view developed.
SICR-5	Retrieve filtered information	The search should enable the filtering of information.	The search has a filter function as well as a graph view to receive filtered information.
SICR-2	Support for Searching	The search should give support in finding documents.	The search supports the user in finding documents. There are various mechanisms implemented and analysed to point user to relevant documents, i.e. translation functions, abstract generation, topics, or the graph view functionality.
SICR-123	Ensure conceptual and linguistic transparency of the inventory	The search should allow a translation of parts of the content.	This requirement was taken into account in the implementation of the search functions and the availability of a translation of abstracts.
SICR-120	Enable direct communication between users	The Search will allow to contact authors of documents.	All search results include a contact of the authors of a document or data source and Therefore, enable direct communication. Other communication option are provided in the interactive platform.
SICR-114	Support inclusiveness through search	The search should enable the filtering of results concerning different regions and actions the users wants to perform.	The search enables the filtering concerning different processes the user is looking for. The regional filtering is not implemented yet, but could easily be implemented if needed.
SICR-107	Support compliance with data minimisation principles	The search will provide compromised information.	The search enable the users a first look on the content of the documents via the defined topics and an abstract of the document. For that reason the data is presented in an optimised way.
SICR-101	Support users in balancing democratic interactions with clear	Reject – this is a question that should be defined by the managing authority and not by the search.	



	chains of command		
SICR-14	Author of Information	The search will provide information about the author of a document.	The search provides information about the author of a document
SICR-32	Size: sufficient but not hindering the process	The search should allow to adjust the amount of search results.	<p>To regulate the kind and amount of search results filters are defined.</p> 
SICR-25	Indicate data quality through supporting data accuracy	The search will define a process to enable high data quality	The process to ensure data quality is described in section 6.1.4 in this deliverable.
SICR-111	Support practices of managing privacy or Design FOR privacy	The search should allow user to restrict access to documents.	When contributing information to the search there is the ability to restrict data. Further guidance is developed in WP2 to cover issues on access restrictions.
SICR-112	Alert users to danger of unlawful re-identification	Reject	Further guidance is developed in WP2 to cover issues on access restrictions and unlawful re-identification.
SICR-121	Support people in lessons learnt reporting so that this	The search should allow to provide new lessons learned.	Lessons Learned are a main point in the analysis of past disasters. The database is editable by end-user.



	does not lead to blame		
SICR-29	Provide information about restricted data?	The search should provide information about restricted data	<p>Restricted documents are seen in the search but not accessible. Therefore, user know about the existence of information.</p> 
SICR-5	Retrieve filtered information	The search will provide filtered data.	<p>The search filters information and documents regarding the entered search word. Therefore, various ontologies are used to try to define the optimal data with regard to the current need of the user. Further the search system provide the possibility to use filter in on the right side of the system to reduce the outputs of the current search process.</p> 
SICR-182	Prompt users to consider privacy, anonymisation and access restrictions	The search should allow user to restrict access to documents	<p>When contributing information to the search there is the ability to restrict data. Further guidance are developed in WP2 to cover issues on access restrictions.</p>



9 Literature index

- [Alde84] Aldenderfer, M.; Blashfield, R.: Cluster Analysis, (1984), pp. 4-15
- [Bair10] Baird, Malcolm E.: The ' Phases ' of Emergency Management. Online: <http://www.vanderbilt.edu/vector/research/emmgtpases.pdf>, 2010.
- [BAZZ09] Baharosa, Nitesh; Appelman, Jaco; Zanten, Bart van; Zuurmond, Arre: Identifying and confirming information and system quality requirements for multi-agency disaster management. In: *Proceedings of the 6th International ISCRAM Conference* (2009), Nr. May, pp. 1–10, ISBN 9789163346040
- [BFV13] Bayrischer Fussball-Verband: Sicherheitskonzept Saison 2012/2013: Mindestanforderungen an das Sicherheitskonzept für Verbandsspiele der Regionalliga Bayern (2013)
- [Data00] Data.gov: Disasters. Online: <https://www.data.gov/disasters/>. (retrieved 2017-01-21)
- [DFB09] Deutscher Fußball-Bund (DFB): Stadionhandbuch: Anforderungen an Fußballstadien in baulicher, infrastruktureller, organisatorischer und betrieblicher Hinsicht. Online: http://www.mik.nrw.de/fileadmin/user_upload/Redakteure/Dokumente/Themen_und_Aufgaben/Schutz_und_Sicherheit/NKSS/Anlagen_Konzept_NKSS_2012/NKSS_A3_DFL_DFB_Stadionhandbuch_20090119.pdf (2009)
- [Dorn94] Dorn, B.: Das informierte Management – Fakten und Signale für schnelle Entscheidungen. Springer Verlag, (1994)
- [Euro07] European Commission: Operations Facility : for a coordinated management of public health emergency at EU level. Online: http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf (2007)
- [FIFA16] FIFA: FIFA-Reglement für Stadionsicherheit. Online: http://de.fifa.com/mm/document/tournament/competition/51/53/98/safetyregulations_d.pdf (2016)
- [Füer14] Füermann, Timo: Was ist eigentlich ein Prozess? In: Prozessmanagement: Kompaktes Wissen, konkrete Umsetzung, Praktische Arbeitshilfen : Carl Hanser Verlag München, (2014), ISBN 978-3-446-43858-3
- [FwDV100] Dienstvorschrift (German Regulation) DV-100 Leadership and Command in Emergency Operations. Online: http://www.idf.nrw.de/projekte/pg_fwdv/pdf/fwdv_100_engl_org.pdf, 2007.
- [FwIS03] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.3), 2015.



- [FwIS04] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.4), 2015.
- [FwIS05] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.5), 2015.
- [FwIS06] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.6), 2015.
- [FwIS07] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.7), 2015.
- [FwIS08] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.8), 2015.
- [FwIS09] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.9), 2015.
- [FwIS11] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.11), 2015.
- [FwIS13] Führungsstab Feuerwehr S 2 (Athanassios Thanos), Feuerwehr Dortmund Mitarbeiterinformation: Flüchtlingslage Nr.3 (fire department Dortmund staff information sheet Nr.13), 2015.
- [GuBe02] Guha-Sapir, Debarati; Below, Regina: The Quality and accuracy of disaster data : A comparative analyse of three global data sets (2002)
- [HaHa14] Handbook, UNHCR Emergency: Common operational datasets (CODs) and fundamental operational datasets (FODs) (2014), pp. 1–4
- [HCLL10] Hristidis, Vagelis; Chen, Shu-Ching; Li, Tao; Luis, Steven; Deng, Yi: Survey of data management and analysis in disaster situations. In: Journal of Systems and Software vol. 83, Nr. 10, (2010), pp. 1701–1714, ISBN 0164-1212
- [Huma00] Humanitarian, Response: Data: Humanitarian Data Exchange. Online: <https://www.humanitarianresponse.info/applications/data/terms-use>. – (retrieved 2017-01-21)
- [Iasc10] IASC: IASC Guidelines Common Operational Datasets (CODs) in Disaster Preparedness and Response. In: *Quality Assurance* (2010), pp. 1–5
- [ICS] Incident Command System. Online: <https://training.fema.gov/emiweb/is/icsresource/assets/reviewmaterials.pdf>, (2008)



- [Inter99] International Standard ISO/IEC:11179-1: Information technology - Specification and standardisation of data elements. Part 1: Framework for specification and standardisation of data elements. Online: [https://www.oasis-open.org/committees/download.php/6233/c002349_ISO_IEC_11179-1_1999\(E\).pdf](https://www.oasis-open.org/committees/download.php/6233/c002349_ISO_IEC_11179-1_1999(E).pdf) (1999)
- [ISO11] ISO 22320:2011(E): Societal security — Emergency management — Requirements for incident response, (2011)
- [MBKB15] Marinova, Silvia; Bandrova, Temenoujka; Kouteva-Guentcheva, Mihaela; Bonchev, Stefan: Thematic Mapping for Disaster Risk Assessment in Case of Earthquake (2015)
- [MBP04] Moll, K.; Broy, M.; Pizka, M.; Seifert, T.; Bregner, K.; Rausch, A.: Erfolgreiches Management von Software-Projekten. Informatik Spektrum 18. Oktober 2004
- [Mert09] Mertens, P. (2009): Schwierigkeiten mit IT-Projekten der öffentlichen Verwaltung. Informatik Spektrum, 18. December 2008
- [NIMS] U.S. Department of Homeland Security: “*National Incident Management System*”. Online: https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, (2008)
- [PBBT14] Petersen, Katrina; Buscher, Monika; Becklake, Sarah; Thomas, Vanessa; Easton, Catherine; Liegl, Michael; Leventakis, Giorgos; Tsoulkas, Vasilis: Overview of Disaster Events, Crisis Management Models and Stakeholders. SecInCoRe Deliverable 2.1, (2014)
- [PKB55] Kent, A; Berry, M.M.; Luehrs, F.U.; Perry, J.W. Machine literature searching VIII. Operational criteria for designing information retrieval systems (1955)
- [SCMW05] Svensson, Stefan; Cedergårdh, Erik; Mårtensson, Ola; Winnberg, Thomas and the Swedish Civil Contingencies Agency: Tactics, command, leadership. Online: <https://www.msb.se/RibData/Filer/pdf/24857.pdf>, (2005)
- [SG01] Standish Group International, Inc. Collaborating on Project Success. Software Magazine, February/March 2001, Wiesner Publishing.
- [TsBG06] Tschoegl, Liz; Below, Regina; Guha-Sapir, Debarati: An analytical review of selected data sets on natural disasters and impacts. In: Proceedings of the UNDP/CRED Workshop on Improving Compilation of Reliable Data on Disaster Occurrence and Impact, Bangkok, April 2006 (2006), pp. 1–21
- [Warf] Warfield, Corina: The Disaster Management Cycle. Online: http://www.gdrc.org/uem/disasters/1-dm_cycle.html (retrieved 2017-01-21)
- [Xu09] Xu, R.; Wunsch, D.: Clustering, (2009), pp.3-9
- [XuZI07] Xu, Wei; Zlatanova, Sisi: Ontologies for disaster management response. In: *Geomatics Solutions for Disaster Management* (2007), pp. 185–200,



ISBN 978-3-540-72108-6

- [York88] York, P. Freund: Critical success factors. Planning Review, Vol. 16, Iss. 4, (1988), pp. 20 – 23
- [ZSTL10] Zheng, Li; Shen, Chao; Tang, Liang; Li, Tao; Luis, Steve; Chen, Shu-Ching; Hristidis, Vagelis: Using data mining techniques to address critical information exchange needs in disaster affected public-private networks. In: Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '10 (2010), ISBN 9781450300551

Internet sources

- [www1] <http://www.mik.nrw.de/themen-aufgaben/auslaenderfragen/asylbewerber/aktuelle-situation-unterbringung/verfahren.html>
- [www2] <http://www.unhcr.org/55dc749d6.html>
- [www3] <http://www.computerwoche.de/a/gescheiterte-it-projekte,2546218>
- [www4] <http://www.spiegel.de/wirtschaft/soziales/grossprojekte-in-deutschland-die-top-und-flop-ten-a-1033977.html>
- [www5] <http://www.businessdictionary.com/definition/key-success-factors.html>
- [www6] <http://www.businessdictionary.com/definition/critical-success-factors-CSF.html>
- [www7] <http://edu-net.nl/Diversen/GRIP.pdf>
- [www8] https://en.wikipedia.org/wiki/Hyponymy_and_hyponymy
- [www9] <https://www.iso.org/obp/ui/#iso:std:iso:19115:-1:ed-1:v1:en>
- [www10] <http://www.preventionweb.net/risk/datasets>
- [www11] <http://data-planet.libguides.com/dataterminology>
- [www12] <https://stats.oecd.org/glossary/detail.asp?ID=542>
- [www13] <http://wirtschaftslexikon.gabler.de/Definition/prozess.html>
- [www14] <http://www.emsa.europa.eu/>
- [www15] <http://ecdc.europa.eu/en/Pages/home.aspx>
- [www16] <http://ec.europa.eu/echo/>
- [www17] http://ec.europa.eu/echo/what/civil-protection_en
- [www18] http://ec.europa.eu/echo/what-we-do/civil-protection/european-medical-corps_en
- [www19] <https://ec.europa.eu/jrc/en>
- [www20] <https://www.europol.europa.eu/>



- [www21] <https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena>
- [www22] http://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/rapid_alert_en
- [www23] <https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system>
- [www24] <https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-platform-for-experts>
- [www25] http://ec.europa.eu/echo/what/civil-protection/mechanism_en
- [www26] <https://www.euractiv.com/section/justice-home-affairs/news/eu-maritime-agency-gets-ready-to-use-drones-to-monitor-refugee-boats/>
- [www27] http://ec.europa.eu/echo/refugee-crisis_en