



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

Deliverable 3.2

First publication of inventory results

Final Version

Steffen Schneider¹, Jens Pottebaum¹, Christoph Amelunxen¹, Maïke Kuhnert², Katrina Petersen³, Monika Büscher³, Andrea Nicolai⁴, Paul Hirst⁵, Ioannis Daniilidis⁶,

¹University of Paderborn, ²Technical University Dortmund, ³Lancaster University, ⁴T6 ECO, ⁵British APCO, ⁶Center for Security Studies (KEMEA)

March 2015

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		13/03/2015		
Sent to coordinator		11/03/2015		
No. of document		D3.2		
Name		<i>First publication of inventory results</i>		
Type		<i>Report</i>		
Status & Version		<i>Final Version 1.0</i>		
No. of pages		63		
Work package		3		
Responsible		<i>UPB</i>		
Further contributors		<i>TUDO T6 ECO ULANC BAPCO KEMEA</i>		
Keywords		<i>inventory results, data sets, command systems, process analysis, information systems, business models, workshop, questionnaire</i>		
History	Version	Date	Author	Comment
	V0.1	11/11/2014	UPB	Draft structure
	V0.2	21/11/2014	UPB	
	V0.3	28/11/2014	UPB	
	V0.4	05/12/2014	UPB	
	V0.5	22/12/2014	UPB	
	V0.6	12/01/2015	UPB/TUDO/ ULANC/BAPCO /KEMEA	Gathering of input
	V0.7	21/01/2015	UPB	Adjustment of input
	V0.8	27/01/2015	UPB/T6	



V0.9	03/02/2015	UPB	
V0.10	06/02/2015	UPB	Preparation for review
V0.11	06/02/2015	UPB	
V0.12	17/02/2015	UPB, TUDO, BAPCO	Adjustments according to the reviews of TUDO and BAPCO
V0.13	04/03/2015	ULANC, UPB	Update after ELSI monitoring review
V0.14	06/03/2015	UPB	Finalisation for 2 nd review
V0.15	09/03/2015	ULANC, TUDO, BAPCO, UPB	Inclusion of review
V1.0	12/03/2015	UPB	Final Edits and submission

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

	<p>University of Paderborn C.I.K.</p>	<p>Steffen Schneider Email: st.schneider@cik.upb.de Jens Pottebaum Email: pottebaum@cik.upb.de Christoph Amelunxen Email: amelunxen@cik.upb.de</p>
	<p>TU Dortmund CNI</p>	<p>Maike Kuhnert Email: maike.kuhnert@tu-dortmund.de</p>
	<p>Mobilities.Lab Centre for Mobilities Research Department of Sociology Lancaster University LA1 4YD UK</p>	<p>Monika Buscher Email: m.buscher@lancaster.ac.uk Katrina Petersen Email: k.petersen@lancaster.ac.uk</p>
	<p>T6 Ecosystems</p>	<p>Andrea Nicolai Email: a.nicolai@t-6.it</p>
	<p>British APCO</p>	<p>Paul Hirst Email: paul.hirst@bapco.org.uk</p>
	<p>Center for Security Studies (KEMEA) P.Kanellopoulou 4 1101 77 Athens Greece</p>	<p>Ioannis Daniilidis Email: i.daniilidis@kemea-research.gr</p>



Reviewers

 <p>tu technische universität dortmund</p> 	TU Dortmund CNI	Mohamad Sbeiti Email: Mohamad.sbeiti@tu-dortmund.de
 <p>BRITISH APCO</p> <p>Knowledge Exchange for Public Safety Communications</p>	British APCO	Paul Hirst Email: paul.hirst@bapco.org.uk



Executive summary

This deliverable describes the first collection of inventory content gathered in WP3. 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, online surveys, and identification of already existing background in the consortium. These activities were complemented by several interactions with stakeholder groups, like the Co-Design/Advisory Board workshop in Manchester and a pilot questionnaire at the Border Surveillance and Search and Rescue symposium in Crete.

The respective results of all these activities are presented in the different chapters of this deliverable and comprise a first version of the inventory content.

One major issue of research in this work package are **data sets**. As described in the research programme for this work package (see deliverable D3.1 [5]), initially information of used and available data sets was gathered and analysed:

- For the analysis of the availability, usage and sharing of data sets, respective sets were collected for two specific regions, namely, Dortmund and San Diego. Analysis shows that there are many different data sources that could be useful in different disaster events. Upcoming WP3 activities are designed to generalise data types in order to draw a generically useful disaster information map, possibly diversified according to different kinds of disaster events.
- In order to identify already existing databases and systems, a list of necessary data sets and respective databases comprising those of the UK was elaborated. It shows that there are many different application areas and databases with different data sets. But it also reveals that there exist databases and systems which include nearly the same set of data and thus may be merged.
- Additionally to the analysis of used, known and needed data sets, SecInCoRe will also consider available, but as of yet unknown or unused data sets. Therefore we are carrying out research on linked open data as machine readable and structured (as linked) data sets. Besides this kind of data the linkage is important to derive first conclusion regarding data networks for modelling taxonomy.
- In order to consider the stakeholders' perspective, a questionnaire was developed and a pilot was distributed at the Border Surveillance and Search and Rescue (BSSAR) symposium in Heraklion. This includes questions regarding data sources, data sharing, data usage, and its acquisition. The small set of answers gathered in the pilot is listed and described in this deliverable. One main conclusion is that the Internet is a tool utilised by all agencies under all operations, in contrast to other channels; this emphasises the importance for the availability of a network / cloud where information can be accessed in order to assist agencies in a pan-European environment.
- These activities in close collaboration with stakeholders were complemented by a special session regarding actually used and required data and information at the Co-Design/Advisory Board workshop in Manchester on 9.-10. December



2014. The outcomes are lists describing the utilisation and demands on different data types, potential sources for provision of these data as well as purposes for using these data. This allowed deriving first conclusions on these topics from different perspectives (overarching both organisation and region).

Another category is **command systems including information management processes**. To address this, the following activities have been undertaken:

- An important issue of this project is the analysis and modelling of command systems and information management processes. In SecInCoRe, a mix of top-down and bottom-up approach is followed in order to enable different techniques (e.g., research on regulations as top-down and interviews as bottom-up), which will lead to a compressed and valid description.
- This approach was applied to analyse the ISO 22320:2011 “*Societal security - Emergency management - Requirements for incident response*” and on the FwDV100. The deliverable comprises first results in this area. Next steps are the ongoing recording and modelling of current processes. The identification of differences and commonalities will lead to a unified command system, which will represent the reference process.

This work package also considers the collection and analysis of **information and communications systems**:

- In order to derive a first overview of current systems, a survey has been started. Key characteristics of information systems have been identified and we have constructed a model database for gathering information regarding the systems categorised by these characteristics. Based on this, a survey was conducted resulting in the collection and description of more than 60 systems. As the picture is constantly changing (e.g., in the UK, Airwave will be replaced with LTE technology in the next few years) the survey is ongoing so that an inclusion of further systems is expected here.
- Another important issue for information systems is categorisation. As described in the Document of Works [3], research in the area of information system paradigms and architectures has been initiated for addressing this issue. In a first step, existing paradigms in the field of software engineering are presented and will be analysed in upcoming activities. In addition to this top-down approach, an analysis of already existing information systems regarding their architecture has been performed. Therefore, current systems have been researched and respective architectures are listed in this deliverable. Like the top-down analysis this bottom-up approach will be ongoing in SecInCoRe.
- Another important aspect of SecInCoRe regarding the analysis of information systems lies in the research on communication systems and data exchange models. As most of these activities, respective efforts are ongoing.

All these activities show that there are many things to be considered by researching on information systems. But it also reveals that there are many systems already existing with different characteristics serving several purposes.

One further research item is on **business models** including procurement approaches. In accordance to the extensive research on information systems, research activities



are focused on business models for the application of information systems. One aspect of this is the provision and maintenance of communication infrastructure necessary for most of the information systems. Moreover, three different models for equipment procurement and system maintenance are described and analysed. In addition to this, a cloud based model is presented. Analysis on these aspects is ongoing.

All in all, many activities of gathering content for the inventory as well as analysing current situations and approaches have been conducted so far. In the upcoming months, we will build on these first results and derive more information and conclusions about data sets, command systems and information management processes, information, and communication systems as well as business models and procurement approaches in order to build a broader and more detailed overview.



Table of contents

1	Introduction	11
1.1	Purpose of this document.....	12
1.2	Validity of this document.....	12
1.3	Relation to other documents.....	12
1.4	Contribution of this document.....	13
1.5	Target audience	13
1.6	Glossary	14
1.7	List of figures.....	15
1.8	Structure of the deliverable.....	16
2	First version of data sets	17
2.1	Activities for the acquisition of representative data sets for past disaster events.....	17
2.2	Acquired data sets.....	19
2.2.1	<i>Results based on preceding research.....</i>	<i>19</i>
2.2.1.1	Specific region: Dortmund (Germany)	19
2.2.1.2	Case study: San Diego (USA).....	20
2.2.2	<i>Inclusion of stakeholders background in the consortium.....</i>	<i>21</i>
2.2.3	<i>Analysis of existing data sets and frameworks.....</i>	<i>22</i>
2.2.4	<i>Questionnaire.....</i>	<i>24</i>
2.2.5	<i>Workshop.....</i>	<i>28</i>
3	Command systems and information management processes	31
3.1	Activities to analyse command systems and information management processes	32
3.2	Results of first process analysis and deviations from command systems	36
4	Information systems	38
4.1	Literature research and inspection of available and frequently used information systems.....	38
4.2	Results of these activities	39
4.2.1	<i>First survey on information systems.....</i>	<i>40</i>
4.2.2	<i>Information system paradigms and corresponding architectures.</i>	<i>43</i>
4.2.3	<i>Communication systems and information exchange models</i>	<i>49</i>
5	Business models for the application of information systems	53



5.1	Activities for analysing business models	53
5.2	Analysis of business models for the application of information systems.	53
6	Literature index	61

1 Introduction

SecInCoRe intends to create 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 real-time decision making (performed in Work Package WP2, see [4]).

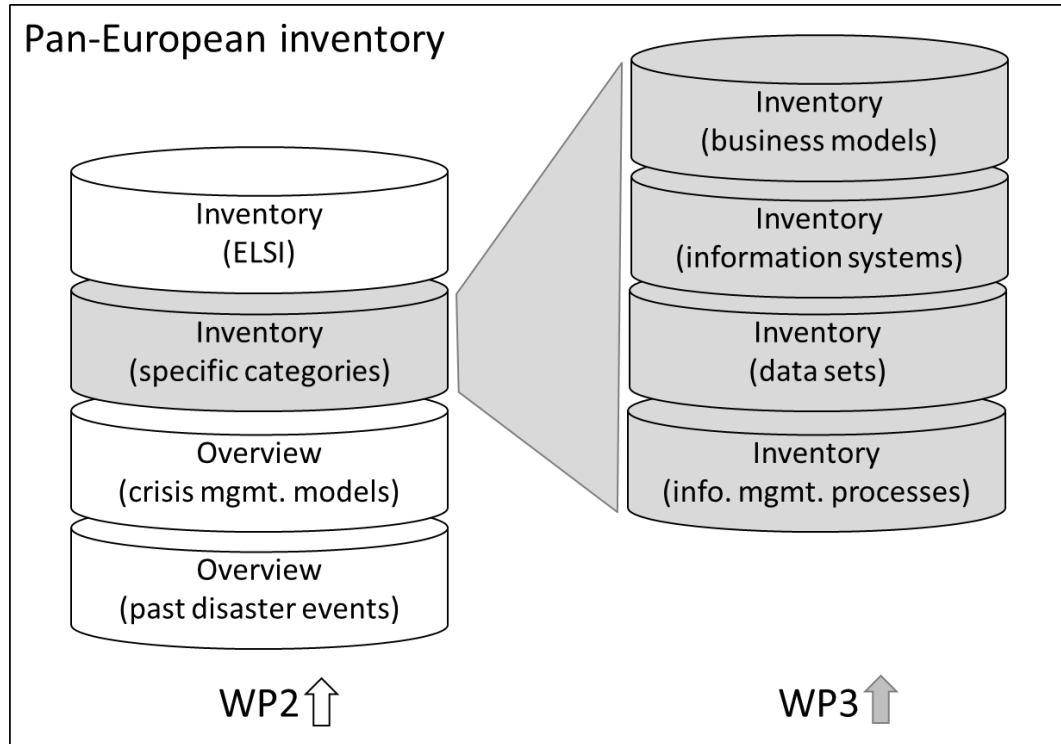


Figure 1 Inventory content

The inventory of disaster events will be complemented by an inventory of related information. According to the high level SecInCoRe objectives (see [3]) and the defined 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 utilise 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, overall crisis management models and lessons learnt within each European country, to point out the possible gaps in data sets, missing interoperability within and between organisations and procedural differences.
- **Information systems:** identification of tools based on information and communication technology (ICT) for data acquisition, processing and provision as well as analysis of success factors and barriers for the application of information systems taking into account available systems (both for daily use and emergency situations) as well as prospective application fields.



- **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 a fit between problems and solutions, a fit between these business models and regional, national, European and even international regulations and public procurement procedures is essential.

1.1 Purpose of this document

This document presents the current 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]), 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

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 have begun to gather and structure inventory content.

1.2 Validity of this document

The deliverable subsumes 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. In the further progress of the project, the input described here will be complemented by means of further studies and research activities. Thus this collection allows just a first overview of data and information of the inventory.

1.3 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

The outputs described in this document build the basis for all activities in WP3 and are therefore related to the following documents directly:

- [6] D3.3 Second publication of inventory results
- [7] D3.4 Final publication of inventory results

As other WPs are connected with respective results, the following documents are also connected to D3.2:

- [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]

All activities in WP3 are based on a strong 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

- [20] D1.2 Research Ethics

1.4 Contribution of this document

This deliverable should facilitate a reflection of the research methodology (as defined in [5]) and first 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]).

Additionally, further stakeholder interactions can be planned and performed envisioning to sustain the inventory as an additional information resource (as part of a Common Information Space, cp. WP4), to build a SecInCoRe community (WP5) and to facilitate to standardisation and harmonisation activities (WP6).

1.5 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 by such kind of experts.

As the categories of the inventory include several differences between each other, some parts of this document address specific reader groups directly (e.g., section 4.2.2 ‘Information system paradigms and corresponding architectures’ is aimed at information system providers and researchers) while they may be hard to understand



by other groups. 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 set 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.

1.6 Glossary

Abbreviation	Expression	Explanation
BPMN	Business Process Model and Notation	Flow chart to model and describe processes
BSSR	“Border Surveillance and Search and Rescue”	Symposium in Heraklion, Crete, which was used for a questionnaire
CAP	Common Alerting Protocol	Data exchange model
DSSA	Domain-Specific Software Architecture	A specific program for an software architecture to make software reusable
EDXL	Emergency Data eXchange Language	Data exchange model
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.
EFAS	European Flood Awareness System	Provides flood forecasting
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
EPC	Event-driven Process Chains	Type of flowchart used for process modelling



Abbreviation	Expression	Explanation
GoF	Gang of Four	The researchers Gamma, Helms, Johnson and Vlissides which elaborated a standard work in software engineering
JRC	Joint Research Centre	The European Commission's in-house science service
LOD	Linked (Open) Data	Web of Data, which can be understood as one realization of the Semantic Web
PPP	Public-private partnerships	Collaboration model between public and private organisations
PRML	Protection and Rescue Markup Language	Data exchange model
RDF	Resource Description Framework	A recommendation for semantic web data models
TSO	Tactical Situation Object	Data exchange model
VCD	Value change diagram	Model to describe processes on a high level detail
	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

1.7 List of figures

Figure 1 Inventory content.....	11
Figure 2 Initial activities for the inventory of data sets	18
Figure 3 Excerpt of the table describing available and used data sets for San Diego.....	21
Figure 4 Excerpt of the list of available and used data sets for UK.....	22
Figure 5 Instance linkages within the linking open data datasets in 2011	23



Figure 6 Responses to the question “Who do you get data from?”	24
Figure 7 Responses to the question “Who do you share data with?”	25
Figure 8 Responses to the question “What data formats do you most commonly use?”	26
Figure 9 Responses to the question “How do you get this data?”	27
Figure 10 Phases in a major incident	28
Figure 11 Excerpt of answers at the Manchester Advisory workshop	30
Figure 12 Research approach for the analysis of command systems and information management (as defined and as maintained in practice)	32
Figure 13 Process and command structure recording, analysis and modelling in WP3	33
Figure 14 Top-down method to analyse command systems (EU)	34
Figure 15 NUTS - National structures (EU) Source: [www2]	35
Figure 16 Current status of activities in task T3.3	38
Figure 17 Database scheme for information systems	41
Figure 18 Characteristics of an IS illustrated exemplary on Euro DMS	43
Figure 19 Hierarchy of structural paradigms acc. to Kaisler	44
Figure 20 Singleton pattern	45
Figure 21 Software architecture concept.....	46
Figure 22 Classification of architectural styles	47
Figure 23 Layered framework architecture.....	48
Figure 24 Excerpt of list regarding Information / Communication Systems and their architecture descriptions	49
Figure 25 Excerpt of the list regarding communication systems.....	50
Figure 26 EDXL and PRML in comparison	52
Figure 27 First activities for analysing business models	53
Figure 28 Cost Dynamics	56
Figure 29 Business Model Evaluation	57

1.8 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 First version of data sets
- Chapter 3 Command systems and information management processes
- Chapter 4 Information systems
- Chapter 5 Business models for to the application of information systems

All these chapters are divided into two major parts: The first part describes all activities undertaken, delineates derivations and similarities to 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 First version of data sets

One major objective of SecInCoRe is an inventory of data sets (Objective 1.2 in [3]). As described in [5] the main focus lies on data usage and exchange during an emergency. Moreover analysis were defined to search for data sets which are

- available and used
- available and shared
- available and not used
- not available but needed
- not available in organisation but in others

In order to address the first two categories, some key questions wer derived to use as a basis for surveys and other enquiries:

- Who/where do you get data from?:
Results of this question can be an organisation (e.g., government organisations like land registry office), a service (e.g., weather services like DWD), a system (e.g., command and control systems like deNIS II^{plus}), a database (like EM-DAT) if possible with its linkage, a place (like operational room) as well as a gathering device (like phone) or a channel (like radio) respectively.
- What data do you get?:
Responses of this question can be a data description of its content (like wind direction and velocity in m/s) as well as its format (like geo-spatial), a data category (like weather data incl. wind data) or data regarding a disaster event (like fire location data)
- How do you use the data?:
Results of this questions can be a detailed description of its purpose (like decision of involving more resources) or a short delineation (plume mapping)
- Who do you share data with?
Responses of this question can be an organisation (e.g., government organisations like land registry office), a service (e.g., weather services like DWD), a system (e.g., command and control systems like deNIS II^{plus}) or a database (like EM-DAT)

The respective different activities to get a first overview about available, used and shared data sets are described in section 2.1 regarding results in 2.2.

2.1 Activities for the acquisition of representative data sets for past disaster events

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

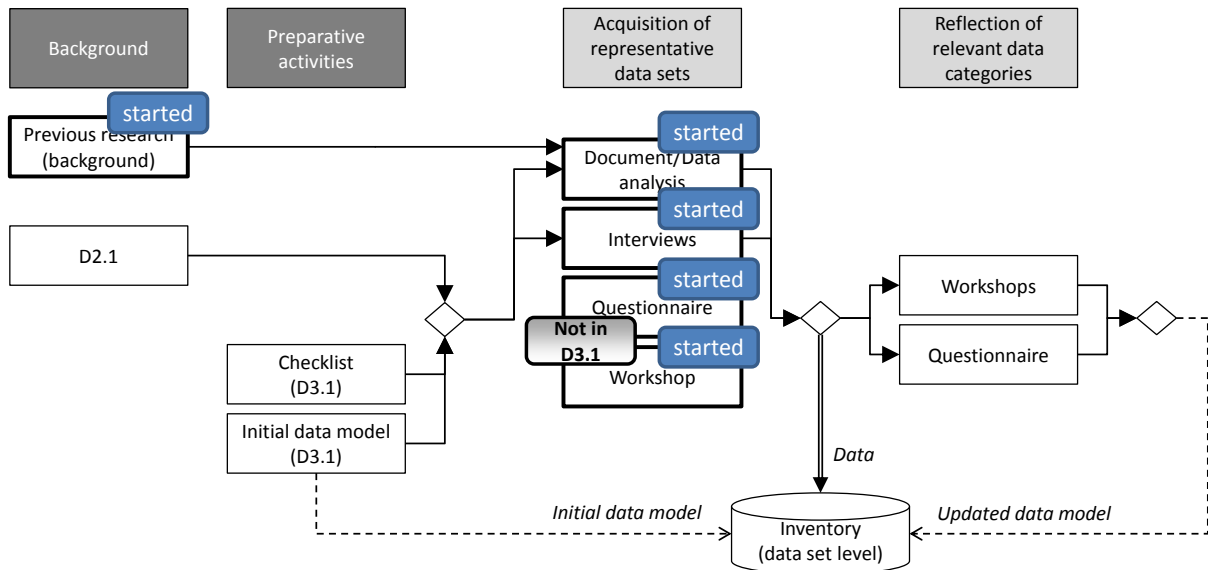


Figure 2 Initial activities for the inventory of data sets

Deviations to the framework are the disposal and analysis of a questionnaire as well as the utilisation of a workshop in order to acquire representative data sets. This change was made for taking the chance of including a stakeholders' perspective during events SecInCoRe members were already participating in. This enables to initiate discussions with respective groups at a very early stage of the project and compare regarding outcomes with those of the other activities planned in [5].

Figure 2 includes all initial activities (marked with blue boxes):

- **Collection and analysis of results from previous research and document / data analysis:** The consortium has access to resources especially regarding data sets used in Germany (several projects, mainly in cooperation with the city of Dortmund) and San Diego (USA). For a first overview lists of available and used data sets were elaborated (cp. section 2.2.1). Moreover BAPCO brought its knowledge into the acquisition by collection data sets used in the UK area (see section 2.2.2). Similar analyses will be done for other regions in the further process of the project. Additionally to that first concepts of linking different data sets were researched on (i.e. linked (open) data, cp. section 2.2.3). This allows both the identification of data sets available as well as the analysis of linkage concepts.
- **Questionnaire and interviews:** In order to gain knowledge about the first responders' and police authorities', perspective questionnaires were prepared and distributed to stakeholder participating to the "Border Surveillance and Search and Rescue" (BSSAR) symposium in Heraklion, Crete on the 27.-28. November 2014. In coordination with the Lancaster University, questionnaires were prepared and distributed to participants of potential stakeholders, such as Duty Officers, Coast Guards, Naval Officers, SAR Operators. The responses have been analysed and are described in section 2.2.4. Besides this questionnaire, KEMEA has been active in the organisation of the interviews, sending invitations to potential stakeholders and end-users. The response has been encouraging and KEMEA will proceed with interviews.



- **Workshops:** Moreover, a first SecInCoRe Co-Design and Advisory Board workshop was conducted on the 9-10 December 2014 in Manchester. Many first responders from different countries participated (see [17]). One main aspect in accordance to the main question regarding data sets was the discussion about what data they use, where it comes from, and which purposes this data usage pursues. The results are presented in this deliverable (see Section 2.2.5) and will build a basis for further analysis in this area.

2.2 Acquired data sets

Based on the different channels (interviews, workshops, etc.) data sets have been acquired. The following section gives a first overview about exemplary results.

2.2.1 Results based on preceding research

For including previous research, available data sets, which are used as information sources for different disaster events, have been collected and are listed for a specific region.

2.2.1.1 Specific region: Dortmund (Germany)

Several research projects have been conducted by the University of Paderborn in cooperation with the Fire Department of Dortmund where Dortmund was subject for case studies in scenario driven research projects. The results are based on interviews, workshops, observations and document analysis. Besides the Fire Department (representing both fire and rescue service), UPB involved several other institutions for these case studies: The technical relief organisation THW, the German Red Cross (DRK), the Police and emergency managers of critical infrastructure operators like Deutsche Bahn. A specific focus on used data types was applied in FP6 IST project SHARE (see [Pott05], [Pott06]), FP7 ICT project PRONTO (see [FPBK09]), German project LAGE (see [LHPK10]) and German project MobisPro (see [KPJ+12]). Data sets subsume the following types

- Resource information
 - Resource characteristics (incl. qualification for personnel)
 - Function in an organisation (personnel, vehicles)
- Documentation from fire protection and prevention processes
- Scenarios for training exercises
- Maps and plans
 - Fire brigade plans
 - Object plans
 - Alarm plans
 - Hydrant plans
 - Sewage plans
- Operational information
 - Operation structure (command levels, hierarchy)



- Representation by tactical symbols
- Incident documentation
 - Incident overview
 - Site map
 - Radio plan and communication sketch
 - Logs (incoming and outgoing messages, status changes, etc.)
 - Recordings (audio, video, various types of sensor data)
 - Debriefing reports

As for the entire document, this is not a complete list of available data sets. The entries are valid not only for Dortmund, but Germany in general.

2.2.1.2 Case study: San Diego (USA)

In a table (see Figure 3) most information sources for disaster events in San Diego are described. The selection of this region is based on two main reasons:

- In San Diego many different data sets exist as open data (accessible for everyone via Internet) which are usable for different purposes and organisations. San Diego County is a productive place to start for gathering such data because the county is large, replete with micro-climates, faces a large number of large-scale emergencies that cross regions of responsibility, and until recently lacked many centralized emergency response agencies (e.g. no centralised fire response), so the organisations within have been innovating ways to encourage interoperability. Thus this first set of information sources can be used as a starting point for drawing an information source map and identifying sensible data sources for other regions.
- In previous work, a first sophisticated current-state-analysis of data set usage and provision has been conducted for the San Diego region. Respective results have been extended and adapted for SecInCoRe. The initial list upon which the below table is based from a pilot project by the San Diego Chapter of the American Red Cross to design a common operating picture/common information space that brings together emergency response organizations (governmental, NGO, etc.) from around the county. The data sets listed are aimed to provide some of the data needed about the region that would be required for decision-making in relation to any organization's response.

The current-state-analysis of information sources for San Diego shows that there exist a lot different data sources which are usable for several disaster events or other purposes. In the next step all data sets will be generalised in order to draw an information map according to different disasters. This allows deriving knowledge about used and needed data sets for specific organisation in a non-regional dependent way. Respective results help to identify information needs and demands as well as available data sets for first responder organisations and police authorities all over the world. Moreover the complete list contains different databases which are usable for other regions, organisations and stakeholders (e.g., the USGS Do you feel it? platform containing several earthquakes all over the world, the Pacific Warning Centre for all



areas with access to the Pacific). Regarding databases will be collected in the inventory to provide an overview about existing information sources for different purposes under specific circumstances (e.g., in case of an earthquake).

Data Type	What For	Where From	Link
<i>FIRE</i>			
Fire location data	current incidents	CalFire	http://cdfdata.fire.ca.gov/incidents/incidents_current
Hazard maps	online hazards map for earthquake, flood, fire, and tsunami	California Emergency Management Agency	http://myhazards.calema.ca.gov/
air pollutants / air quality meteorological data	Plume mapping, health hazard mapping	CA Environmental Protection Agency - Air Resources Board modeling software	http://www.arb.ca.gov/html/soft.htm

Figure 3 Excerpt of the table describing available and used data sets for San Diego

Further activities in this area in the further process of SecInCoRe will target another case study including a similar procedure for another region in Europe in order to compare results and derive more conclusions on data sets used and needed.

2.2.2 Inclusion of stakeholders background in the consortium

One important aspect in the inclusion of background is the utilisation of knowledge of a BAPCO as both a main stakeholder of SecInCoRe and a member of the SecInCoRe consortium. As this includes experience especially for the UK area a first collection of databases and data sets hosted and used in the UK was conducted. The respective result is summarised in a list describing databases, systems and purposes in regard to including data sets (see Figure 4). The results indicate that there are many different application areas and databases with different data sets. But they also confirm that there are databases and systems which include nearly the same set of data and thus may be incorporated. For example, the voters' registers, contact databases and security service systems comprise personal data like names and address and may thus have overlapping entries.



Databases / Systems / Purposes	Data sets	Description / Comments
Command & Control	Times	
	Dates	
	Incident log	Multiple entries from multiple operators and / or locations
	Locations	
	Information <ul style="list-style-type: none"> • Inbound from members of the public • Inbound from other organisations / agencies • Inbound from internal departments 	

Figure 4 Excerpt of the list of available and used data sets for UK

2.2.3 Analysis of existing data sets and frameworks

These efforts lead to a first insight of used data sets. For upcoming activities in Task T3.1 not only those kinds of data sets will be considered. As described in [5 , p. 26f.] also available data sets will be regarded in the further research. In order to follow a holistic approach SecInCoRe takes in respective analysis human to human, human to machine and machine to machine communication into account. To do so SecInCoRe takes automatic methods in consideration. There exist several approaches to enable automatic identification of relevant data available by machines and thus a direct machine to machine communication (semantics, tagging, etc.).

One of those is the concept of Linked (Open) Data (LOD):

“The idea is simple: if we start to publish machine-readable data, such as RDF [Resource Description Framework, a recommendation for semantic web data models; comment by author] documents on the Web, and somehow make all these documents connected to each other, then we will be creating a Linked Data Web that can be processed by machines. [...] This Web of Data, at this point, can be understood as



one realization of the Semantic Web. The Semantic Web, therefore, can be viewed as created by the linked structured data on the Web.” [Yu11, p. 410f.]

An illustration of linkages between different databases and data sources is shown in Figure 5.

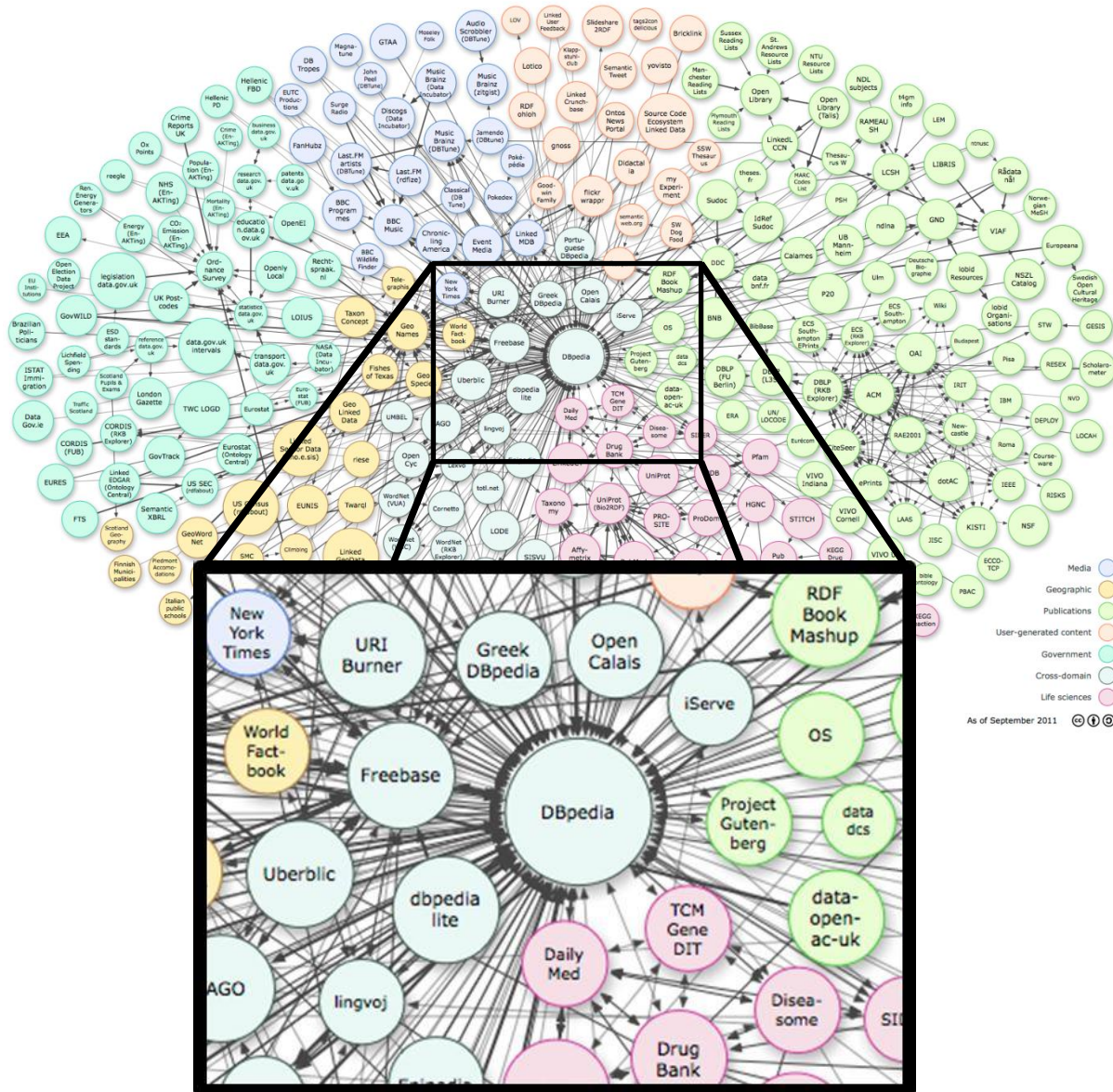


Figure 5 Instance linkages within the linking open data datasets in 2011
Source: Adjusted illustration from [www1]

In the following Task T3.1 of SecInCoRe will analyse existing efforts in this area in order to collect links to machine-readable data in the inventory and to derive connections between different data types. These actions will be followed by further research on other concepts for machine to machine communication and respective data sets relevant for SecInCoRe stakeholders as well as different linkages between different data types.



2.2.4 Questionnaire

The results described above are all based on experience and research background of SecInCoRe members. As emphasised in section 2.1 it is important to include the stakeholders' perspective to assess the current results. Therefore a pilot questionnaire was elaborated and distributed at the Border Surveillance and Search and Rescue (BSSAR) symposium in Heraklion as a preliminary validation of our work until this phase of the project. Though there were only few responses (5) the initial outcomes of the background based activities were confirmed. While two of the questionnaire participants were from duty officers, one was from an On-scene Commander, one from a SAR coordinator, and one from a participant of an agency but who did not want to provide an ID. On basis of the questionnaire a discussion with 5 additional experts working in the same area was performed. The results of the questionnaire and the outcomes of the discussion afterwards were analysed in the following.

As the use and exchange of data sets are focused the phase during an emergency all questions were regarded to this. Moreover all questions are in line with the aforementioned aspects for available, used and shared data formats.

The first question was **“Who do you get data from?”**; the responses are illustrated in Figure 6. The results for example regarding Government Agencies and General Public can be interpreted as follows: While all respondents use data sets from Government Agencies only 30% of them would consider the General Public information pool. From the responses it is obvious that the core source is Government organisations, while Social Media is the second most frequently used source for data, as can be seen from the diagram below. Analytical report of the organisations and media is shown at the table above.

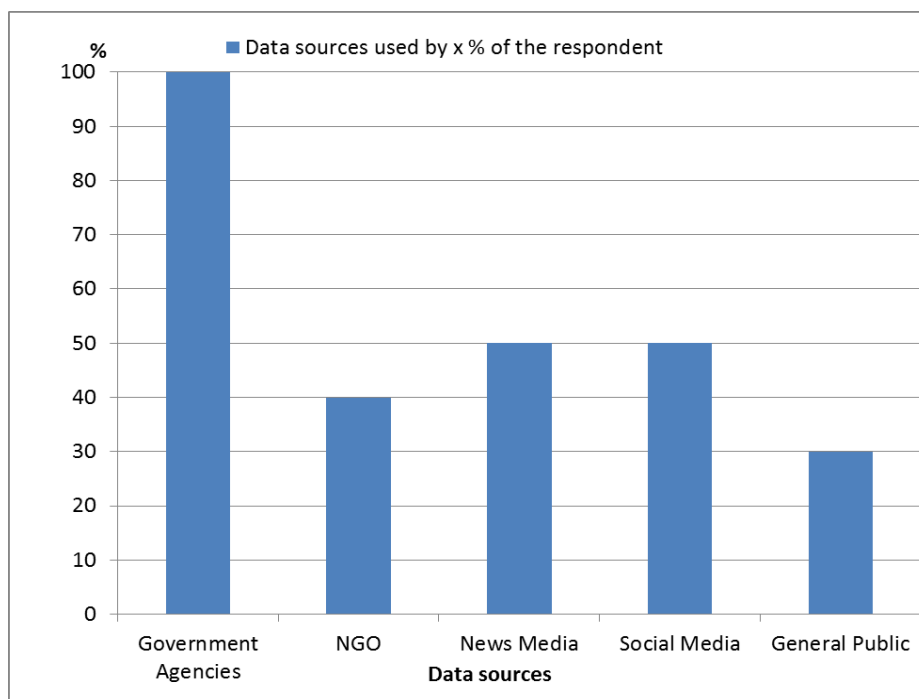


Figure 6 Responses to the question “Who do you get data from?”

As a matter of fact, depending on the nature of the incident other sources, even national or international sources are sought.



The second question is “**Who do you share data with?**” The responses received are listed in Figure 7.

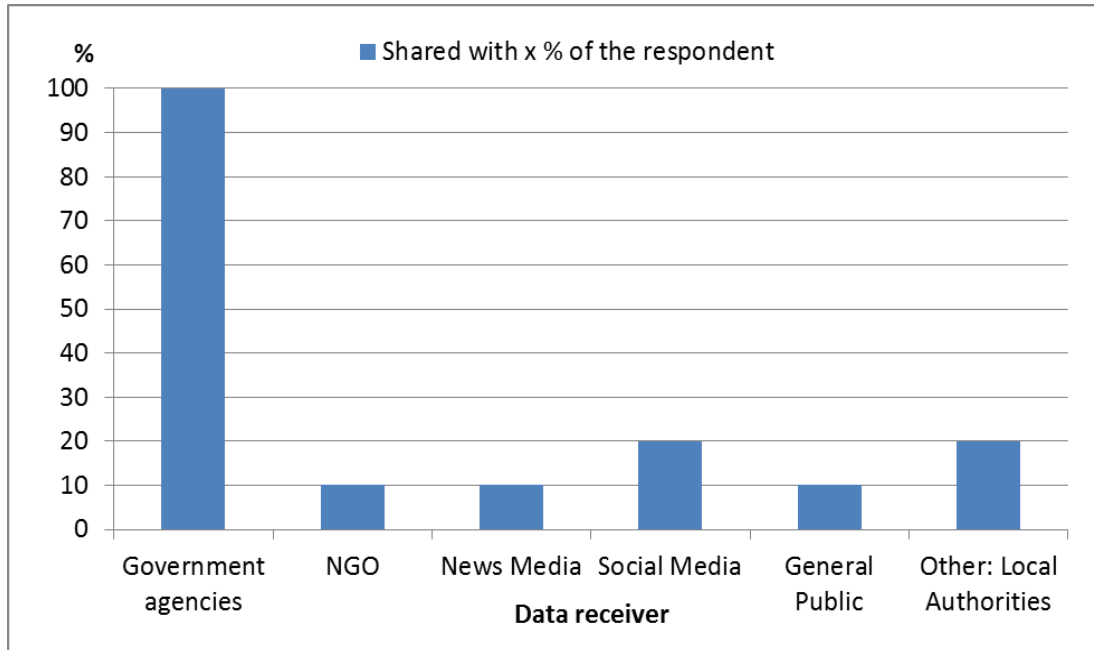


Figure 7 Responses to the question “Who do you share data with?”

Depending on the agency the individuals represented, different priorities are encountered regarding the information that is critical and must be available, shared and the procedure that communicates this information. When crises involve humans, it is emphasised that the Centre for Special Diseases is involved during all operations, being in search and rescue (SaR) of illegal immigrants, but not limited to this. Depending on the spatial orientation of the crisis / disaster event (geographical), data is communicated (inbound/outbound) to neighbouring countries for information that can range from single source (e.g., coast or border guard) to a network of sources.

The third question addressed is: “**What data formats do you most commonly use?**” The results obtained from the analysis of the responses to this question of the participants to the BSSAR questionnaire, a pattern of the most common format of data that is used can be seen to Figure 8.

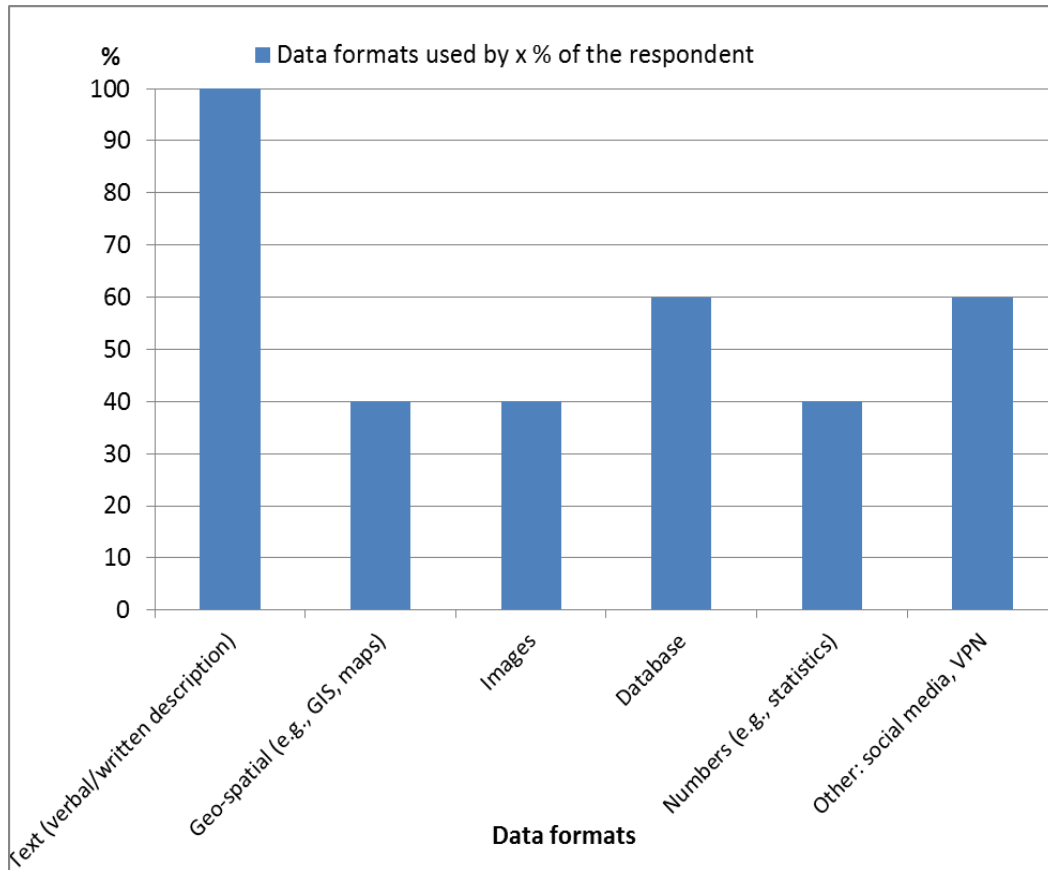


Figure 8 Responses to the question “What data formats do you most commonly use?”

It becomes obvious that the Text (Verbal / Written description) is the format that is used by all participants. The next interesting observation is the increased reliance on data from the social media (Other: Social Media, VPN), a factor that maybe needs to be evaluated to greater depth as to its validity and influence. Of course it is interesting to note the fact that 60% of the responders consider the “Database” a key source of information, a role to be adopted by SecInCoRe, indicating a “mature” target group.

The next question is “**How do you get this data?**” From the analysis of the questionnaire responses regarding methods of data collection during a large scale emergency response, it was a surprise to note that the one standing out is through the Internet, once again stressing the importance of the objective that a program such as SecInCoRe has (see Figure 9).

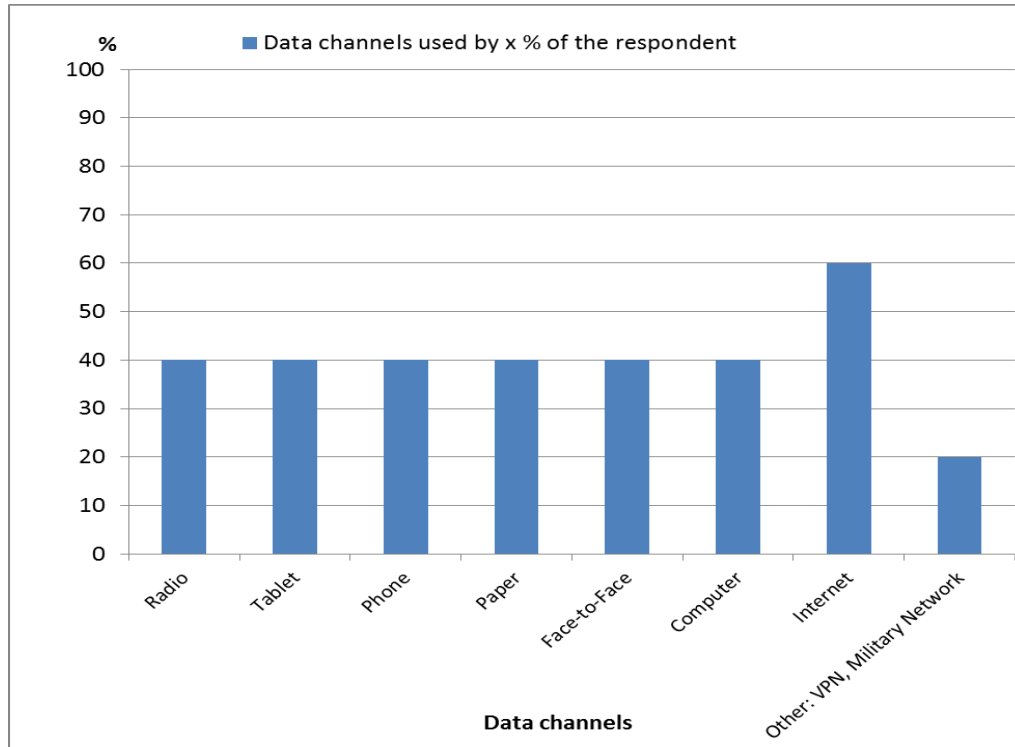


Figure 9 Responses to the question “How do you get this data?”

It is interesting that while there is a uniform methodology for all responders, there is no one method adopted by all, but depending on their operation and nature of agency they represented, different data was used and their value was rated accordingly. For example, the responders from the strictly military agencies were relying mostly on solid sources of the military network and communications and databases, also evaluating the data from the Internet, but did not use normal phone, radio, or tablet at all. Again here, it is obvious that the utilisation of the Internet is a tool that assists all agencies during operations. Another analysis indicates that first responders units utilise all sources available and rely on all formats of data, sourcing from strict access networks to all formats of social media (blogs, Facebook, Twitter etc.). As expected, the collection of information is dynamic and evolves with time, as initially fundamental information is required in order to form the primary data that will assist with the decisions and engagement to handle the crisis. Hence, information answering the basic questions such as “What?, Where?, When?, Who?, How?, and Why?”. These lead to other questions where respective answers enable a more detailed picture of the incident, provide input to the decision-making procedures. Based on the information received during the initial stages of the incident and from the answers of the aforementioned basic questions, planning is organised, weather conditions are defined, asset deployment is set and based on the developing situation and the dynamic data received, decisions are made. The data sets and their evaluation is divided in three stages, the initial phase, during development, and final situation, during all of which data is collected and evaluated until the incident is terminated (cp. Figure 10). Interesting was the single reply by all responders that in cases where information or data is not available, the procedure is based on the data collected on the scene of the incident and then this information is distributed to all parties involved.

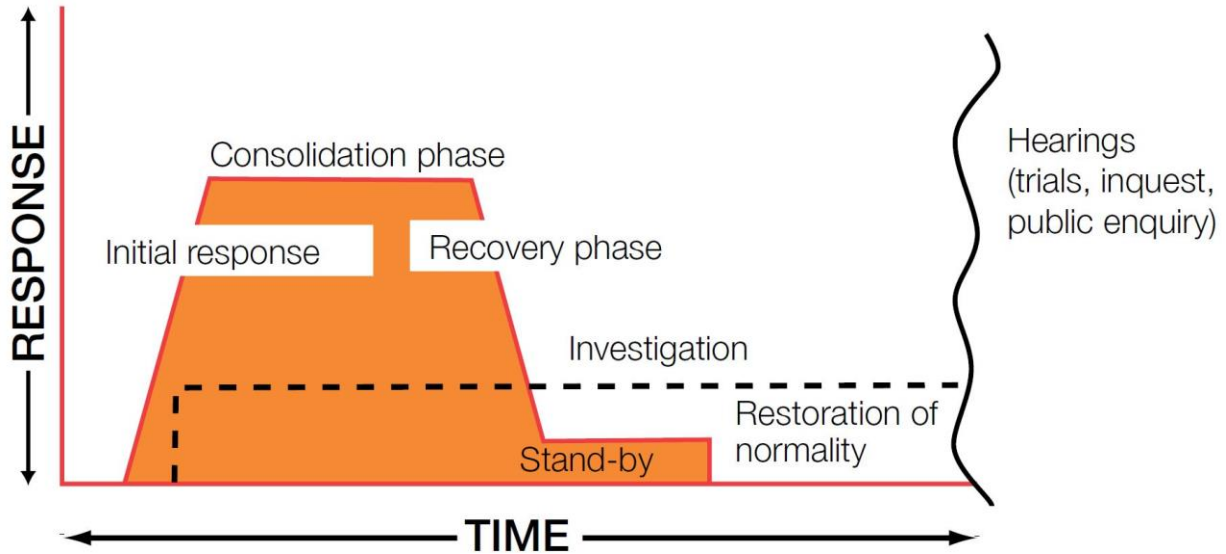


Figure 10 Phases in a major incident
Source: [NN06, p. 4]

As a final remark, it can be concluded from the responses received that the Internet is a tool utilised by all agencies under all operations, in contrast to other channels; this emphasises the importance of the availability of a network where information can be accessed in order to assist agencies in a pan-European environment.

2.2.5 Workshop¹

At the Co-Design / Advisory Board workshop in Manchester on December the 9th and 10th fourteen experts from different first responder organisations and police authorities in Europe as well as eleven members of SecInCoRe discussed the use and meaning of specific data sets. According to the main questions defined to identify available, used and shared data sets, the following three questions were asked:

- What data is used? → Data types
- Where does the data come from? → Data sources and resources
- How do you use it? → Purpose

An excerpt of the answer's collection is as follows:

Category	Entry
Data types	
Meteorological/topological data	Meteorology – current prediction
	Meteorology – current & predicted

¹ The workshop mainly addressed co-design for the SecInCoRe demonstrator (see [17] and [9]). As a side effect, inventory results were created throughout the sessions in this workshop.



Category	Entry
	Meteorology
	Weather conditions
	Weather information
	Height of the emergency (literally how high up is it)
	Exact location
	A location point
...	
Data sources	
Command & Control	Operational room (provisional, regional, national)
	Command and Control
	Central Emergencies Communication Operative
	Internal to the Organisation (Human Resources, Logistics, Legal)
...	
Purpose	
Planning / Decision making	Request resources
	How many resources I have to use
	To involve more resources if necessary
	Deploying resources to best effect
	To know where the emergency is
	To make the prioritisation of the activities
	To define priorities



Category	Entry
	Operational picture
	Gaining strategic overview and ensuring common situational awareness
	Planning to set a strategy
	...

Figure 11 Excerpt of answers at the Manchester Advisory workshop

In some points the perspective on data sets varies between different experts from several countries while there were some aspects which were agreed from all participants. This confirms that different organisation in several regions have to be regarded within the research on the usage of data sets. Systemic process analysis based on unified incident command systems



3 Command systems and information management processes

The command system and the information management processes are closely related since information management is an essential element in command and control. The boundaries are often fluid so that the term “command systems” and “information management” are inextricably linked in this Chapter. Today there are a lot of national, regional or single organisation guidelines, rules, strategies, manuals, etc. They have a wide range of content different levels of detail from abstract to very detailed. In the following a first collection of those is presented:

- International Standard
 - ISO 22320 Societal security — Emergency management — Requirements for incident response
- Germany
 - Feuerwehrdienstvorschrift (German Fire Service Regulation) 100 (FwDV100)²
- USA
 - National Incident Command System (NICS)³
 - Subcomponent: Incident Command System (ICS)⁴
- UK
 - Legislation:
 - Fire and Rescue Services Act 2004⁵
 - Civil Contingencies Act 2004⁶
 - Fire and Rescue Service Operational Guidance e.g.,
 - Risk assessment⁷
 - Health, safety and welfare framework for the operational environment⁸
 - Fire and Rescue Manual⁹
 - Civil Protection Lexicon¹⁰

² see http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/FIS/DownloadsRechtundVorschriften/Volltext_Fw_Dv/FwDV-100%20englisch.pdf?__blob=publicationFile

³ cp. http://www.enviro.ie/en/Publications/Community/FireandEmergencyServices/FileDownload_2099_en.pdf und http://www.dleg.state.mi.us/ccfs/bcc/pdf/dleg_bccfs_manual_nims_ics.pdf

⁴ see <https://training.fema.gov/EMIWeb/IS/ICSResource/assets/reviewMaterials.pdf> und <http://www.epa.gov/watersecurity/tools/trainingcd/trainers/ICS.pdf>

⁵ This Act defines the responsibility areas of Fire & Rescue services (see http://www.legislation.gov.uk/ukpga/2004/21/pdfs/ukpga_20040021_en.pdf).

⁶ cp. http://www.legislation.gov.uk/ukpga/2004/36/pdfs/ukpga_20040036_en.pdf

⁷ see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/9391/1929850.pdf

⁸ cp. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/209362/HSFrameworkJunecombined.pdf

⁹ This is a manual of guidance and not law (see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/7643/incidentcommand.pdf)



- College of Policing – Civil Contingencies¹¹
- Joint Emergency Services Information Programme¹²
- Central Government’s Concept of Operations¹³

For upcoming Tasks it is important to define an approach for analysing and modelling some of these.

3.1 Activities to analyse command systems and information management processes

According to the research framework of D3.1 Inventory Framework several activities have been conducted to analysis the command systems and information management process. The sequence of the packages is variable and is an ongoing mix process. The process modelling part for example depends of the actually information input. As follow the extended figure of the research approach:

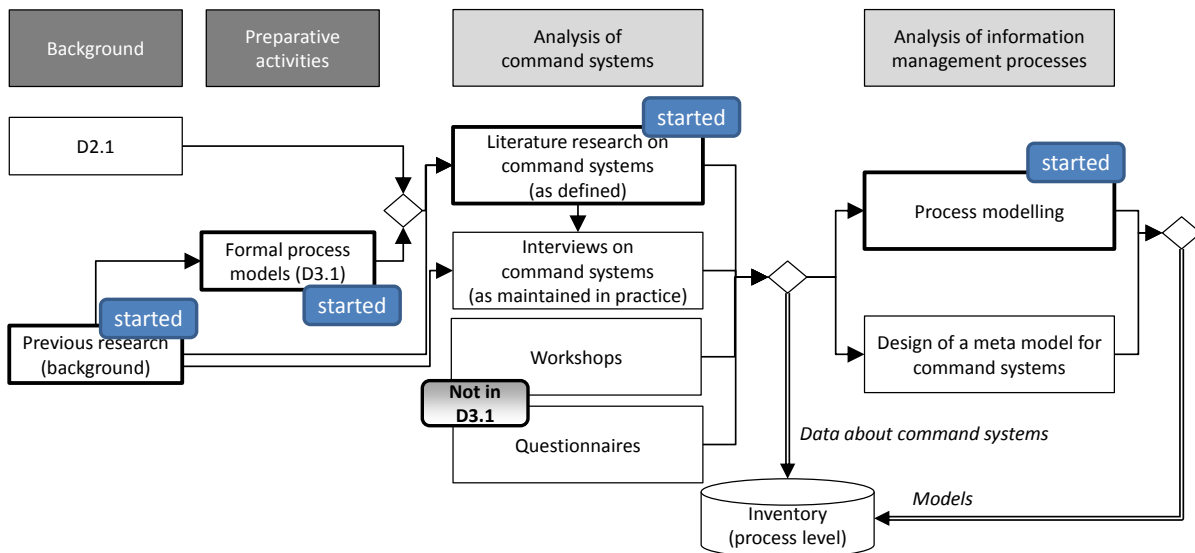


Figure 12 Research approach for the analysis of command systems and information management (as defined and as maintained in practice)
Source: Excerpt from [5 , p. 30]

- **Previous research (background):** The analysis of deliverables and awareness of command systems and information management from previously projects build the foundation of further analysis. Beside the command structure and command process it includes additional information about needed data for first

¹⁰ This describes common understanding of phrases and terminology (see <https://www.gov.uk/government/publications/emergency-responder-interopability-lexicon>).

¹¹ <https://www.app.college.police.uk/app-content/civil-contingencies/>

¹² <http://www.jesip.org.uk/>

¹³ This is a document setting out the arrangements for the response to emergencies requiring co-ordinated UK central government action (see <https://www.gov.uk/government/publications/the-central-government-s-concept-of-operations>).

responders. The project deliverables of past projects are reviewed to relevant information.

- **Formal process models:** The considered model languages are Value chain diagrams (VCD), event-driven process chains (EPC) and Business Process Model and Notation (BPMN). It includes additional the determined symbols, syntax and semantic. Structures are diagrammed in organigrams.
- **Literature research on command system:** It builds the basis of the analysis of command systems and is a start point of process oriented interviews.
- **Process modelling:** Information management process is started to describe in models of command systems which includes process and structure. The analysis is an ongoing process and starts already during the recording and modelling. Additional the analysis identify information which are need according to the process, role and position.
- **Questionnaires and workshops:** Depending of the progress of the command system and information management analysis is could be helpful to make questionnaires and workshop to specific topics or issues. Additional it is useful to connect these actions with the acquisition of data sets. This awareness is a conclusion from the analysis of previous deliverables and the actually research status.

According to [5] the approach to analysis and model the command systems is described as follows:

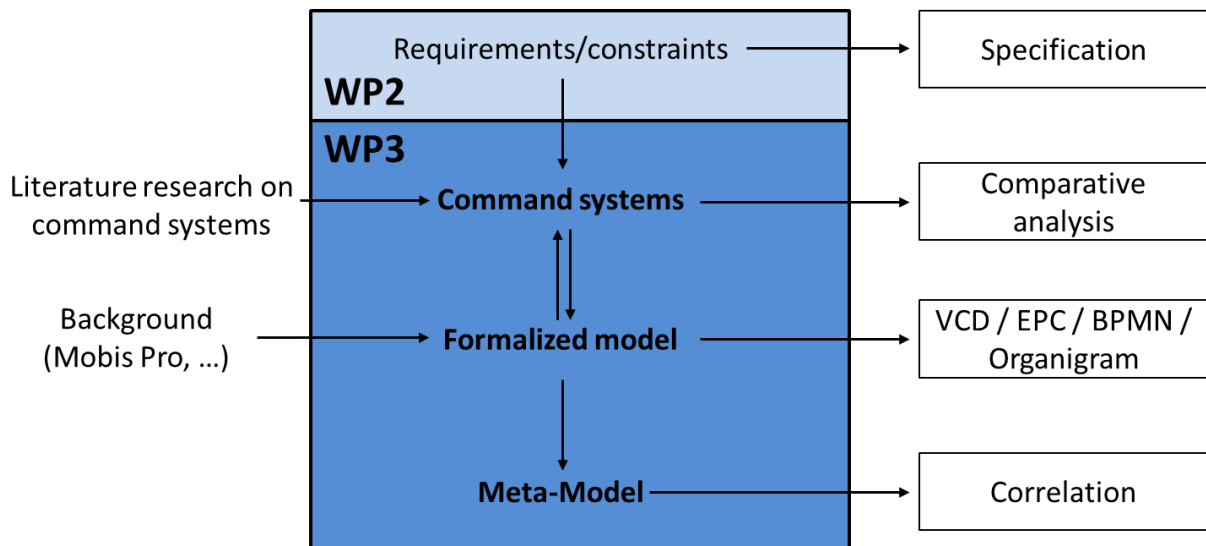


Figure 13 Process and command structure recording, analysis and modelling in WP3
Source: Excerpt from [5 , p. 31]

The analysis of the command systems is the basis to formalise the processes in organigrams, Value Chain Diagrams (VCD), Event-driven Process Chains (EPC) and Business Process Model and Notation (BPMN) models.

The first step is to record the command systems process. Here, in general, exist two important approaches, the top-down and bottom-up approach. In this case a mix of

both methods will be used. The top-down method fragments the processes "from rough to detail". This is useful for example to analyse the processes via literature research. The bottom-up method does not consider the whole process but the sub-process in detail. In the further process the gathered sub-processes are being connected, classified and merged. This method is suitable to record the current process by observations, workshops, interviews or questionnaires. Usually the interviewed persons are know-how bearers in a special part of the whole process. The outcomes of this approach are separate sub-processes.

The next step is to model and analyse the records. It is an ongoing process which will switch between recording, modelling and analysing. At which the recording of the current process is very time-consuming. In Figure 14 the top-down method regarding the analysis of command systems of European countries is diagrammed.

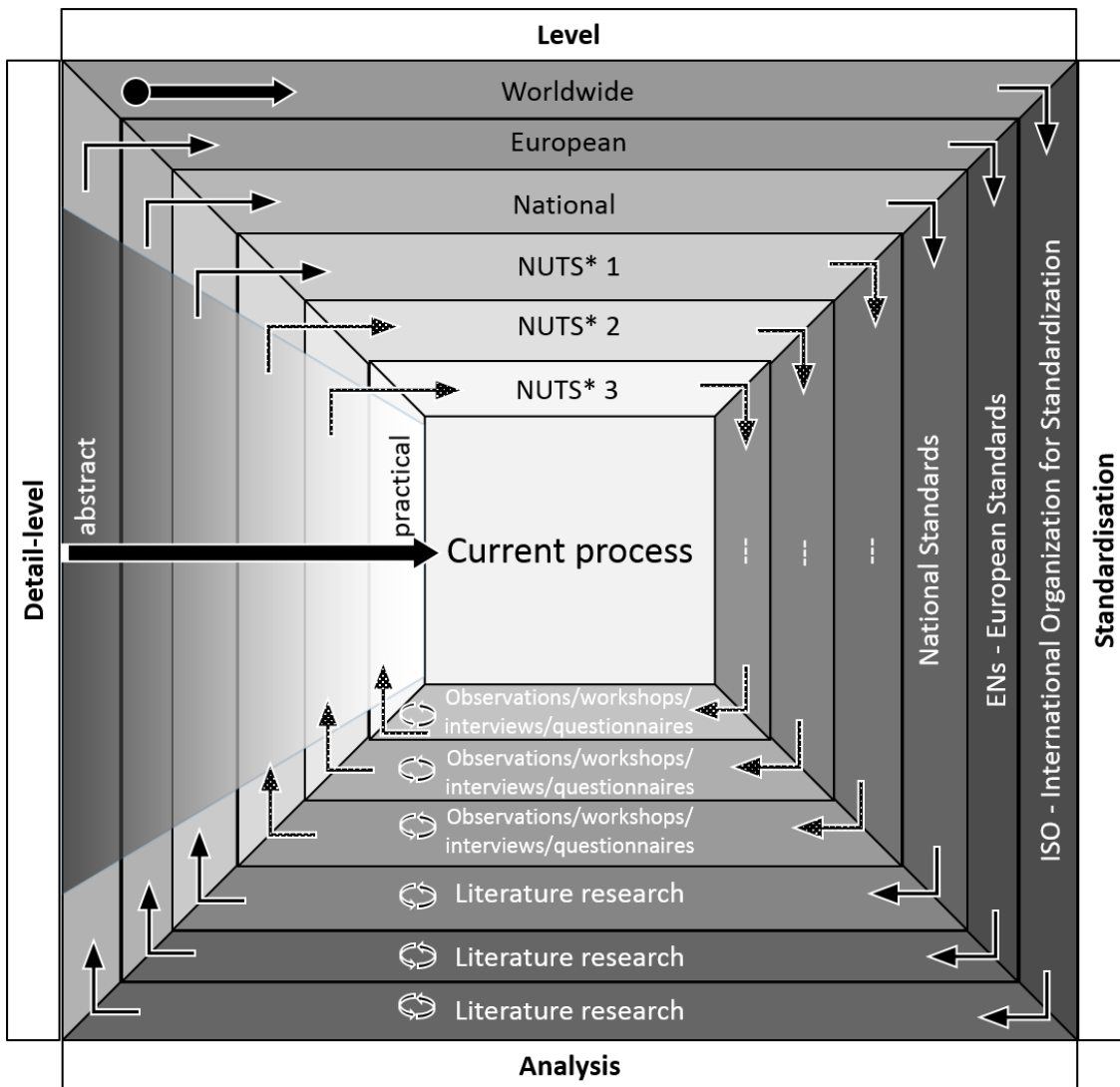


Figure 14 Top-down method to analyse command systems (EU)

The method is symbolised as a pyramid. The basis is represented through the ISO international organisation for standardisation. But there are inter-dependencies



between the different standards. So is for example the DIN Standards Committee for Firefighting and Fire Protection¹⁴ (FNFW) cooperating with the CEN- and ISO-committees, so that there are commonalities between the ISO, CEN and DIN standards.

To define levels for a common basis is an important step. Further it is the foundation for the comparability to describe the process in the different nations. The classification of the first three levels is a result of the standardisation which is described through the validity of the particular standards. To describe the lower levels in a common way for European nation it needs a standard grouping of the regions. For this is made use the classification of the statistical office of the European Union (Eurostat). For dividing up the economic territory of the EU, Eurostat developed the hierarchical system Nomenclature of territorial units for statistics (NUTS). One of its aims is the harmonisation of European regional statistics. This is an approach to harmonise the process. It is classified in [www2]:

- NUTS 1: major socio-economic regions
- NUTS 2: basic regions for the application of regional policies
- NUTS 3: small regions for specific diagnoses

An example for structure of the levels in different EU nations is depicted in Figure 15.

	NUTS 1		NUTS 2		NUTS 3	
DE: Germany	Länder	16	Regierungsbezirke	38	Kreise	412
EL: GREECE	Γεωγραφική Ομάδα	4	Περιφέρειες	13	Νομοί	51
	(Groups of development regions)		(Periferies)		(Nomoi)	
FR: France	Z.E.A.T + DOM	9	Régions + DOM	26	Départements + DOM	100
IT: Italy	Gruppi di regioni	5	Regioni	21	Provincie	110
UK: United Kingdom	Government Office Regions; Country	12	Counties (some grouped); Inner and Outer London; Groups of unitary authorities	37	Upper tier authorities or groups of lower tier authorities (unitary authorities or districts)	139

Figure 15 NUTS - National structures (EU)¹⁵

Source: [www2]

¹⁴ <http://www.fnfw.din.de/cmd?level=tpl-untergremium-ome&languageid=de&subcommitteeid=92707317>

¹⁵ DOM represents “Département d’outre-Mer” and Z.E.A.T. “Zone économique d’aménagement du territoire”.



In the first three levels, worldwide, European and national, it is possible to analyse the documents via literature research with the top-down method.

In the next three NUTS-levels are a lot of national, regional or single organization guidelines, rules, strategies, manuals, etc. They have a wide content range and different levels of descriptions from abstract to very detailed respectively practical. So it is necessary to use a mix of both methods, top-down and bottom-up, to analyse the process at which the second one is dominated.

On the deeper NUTS-levels exist a lot more guidelines, manuals, etc. which describe the process in detail. This descriptions are focused the point of use in relation to the very specific requirements. For example this could be a special command-tactic for a specific building.

Following this common approach for analysis and modelling first results are as succeeding.

3.2 Results of first process analysis and deviations from command systems

The International Organisation for Standardisation (ISO) recognised the national interdependency between organisations and agencies in emergency management. Therefore the Technical Committee ISO/TC 223 developed the ISO 22320:2011 “*Societal security - Emergency management - Requirements for incident response*”.

“This International Standard specifies minimum requirements for effective incident response and provides the basics for command and control, operational information, coordination and cooperation within an incident response organization. It includes command and control organizational structures and procedures, decision support, traceability, information management, and interoperability.

It establishes requirements for operational information for incident response which specifies processes, systems of work, data capture and management in order to produce timely, relevant and accurate information. It supports the process of command and control as well as coordination and cooperation, internally within the organization and externally with other involved parties, and specifies requirements for coordination and cooperation between organizations.” [ISO11, p. 1]

This standard is for all private, public, governmental or non-profit organisations. It includes the requirements for command and control, operational information and cooperation and coordination. The operational information is a part of the command system but they are so important and extensive, that they are described in a separate Chapter. It includes the information process and criteria with requirements to the Quality, Perspective, Synchronisation, Integrity, Coordination and cooperation, Prioritization, Prediction, Agility, Collaboration and Fusion.

The requirements for a command and control system are [ISO11]:

- a command and control structure,
- a command and control process, and
- the resources necessary to implement the command structure and process.

On the national level, for example in Germany, there is the German Regulation 100 “DV-100 Leadership and Command in Emergency Operations”. These regulations are



valid for mission and training in all federal states in Germany. It includes the command system inclusive the means for implementing the incident command. Most of the education in German training schools are basing on the DV-100. Consequently the Fire fighters are working to these rules in their daily work and so in the current process. In the DV-100 the command system is defined as [FwDV100]:

- *command organisation (structure)*
- *command process (procedures)*
- *means to implement the command system (equipment)*

The DV-100 describes the command organisation in detail. Especially the structure and size of incident command in different use cases.

The ISO 22320 and DV-100 have a similar definition of the command system. The content respectively the detail of the description is different. The DV-100 do not describe in detail the operational information like the ISO 22320. Furthermore it does not consider the cooperation between states but it includes the cooperation between different organisation and potential communication.

To analyse the specific processes on the NUTS 2 level it could be useful to support the recording with a technical-system. The Project “RescueLab”¹⁶, with a sub-goal of the automatic recording of training, developed a system to record the important events with diverse technical solutions. Within the Project it was possible to observe amongst others three large-scale exercises of different fire brigades. The first one was with the fire brigade of Dortmund within the realistic scenario “fire in the underground”¹⁷, the second one with a fire brigade at the fire training school of Münster within the scenario “cellar-fire in a multi-story home”¹⁸. The third one was an exercise over three month with different fire brigades at the fire training school in Frankfurt am Main¹⁹. The last one includes four different smaller exercises which are repeated with every fire brigade in a tactical unit of nine fire fighters.

With this solution it could be possible to have a good support to analysis the current command processes respectively the information flow in an incident response. And further the deviations from the unified command systems. Differences in the processes between unified and current could have effects on the information flow and demand.

The next steps are the ongoing recording and modelling of the current command processes. The differences and commonalities have to be identified to derive a unified command system which will represent the reference process.

¹⁶ IT-Supported Training Environments for Civil Protection- and Rescue Forces (<http://www.cik.uni-paderborn.de/en/research/public-security-safety/rescuelab/>)

¹⁷ <http://www.cik.uni-paderborn.de/aktuelles/brand-in-der-u-bahn/>

¹⁸ <http://www.cik.uni-paderborn.de/aktuelles/meilenstein-2-rescuelab/>

¹⁹ Tactical and strategic Innovative Fire protection on the basis of risk-based optimizations (<http://www.feuerwehr-frankfurt.de/index.php/projekte/tibro>)



4 Information systems

One major task of first responders within an emergency lies in giving efficient aid immediately. Those activities demand the capability to make right decisions on the basis of adequate information. The requirement of acting fast and appropriately to protect people and assets is becoming more complex due to more and more information available. Though communication speed up on the basis of new exchange standards, different information channels demand an adequate management of information flows. Thus, information and communication technologies (ICT) are needed for the distribution of relevant information to persons responsible in an incident. Since there exist multiple different information systems addressing first responders for that purpose, the selection of a suitable system is quite difficult.

Consequently, the development of an overview over existing information systems and their special characteristics helps to understand the system topography as well as to identify the availability, usage and exchange of data. Moreover it enables a comparison of different applications and the derivation of success factors and barriers. Therefore, the inventory includes an overview comprising a short description of the system, its special features, organisations to be addressed, and interfaces to other systems.

4.1 Literature research and inspection of available and frequently used information systems

The approach for research in this area was defined in [5]. In accordance to this respective activities have already been started (see Figure 16).

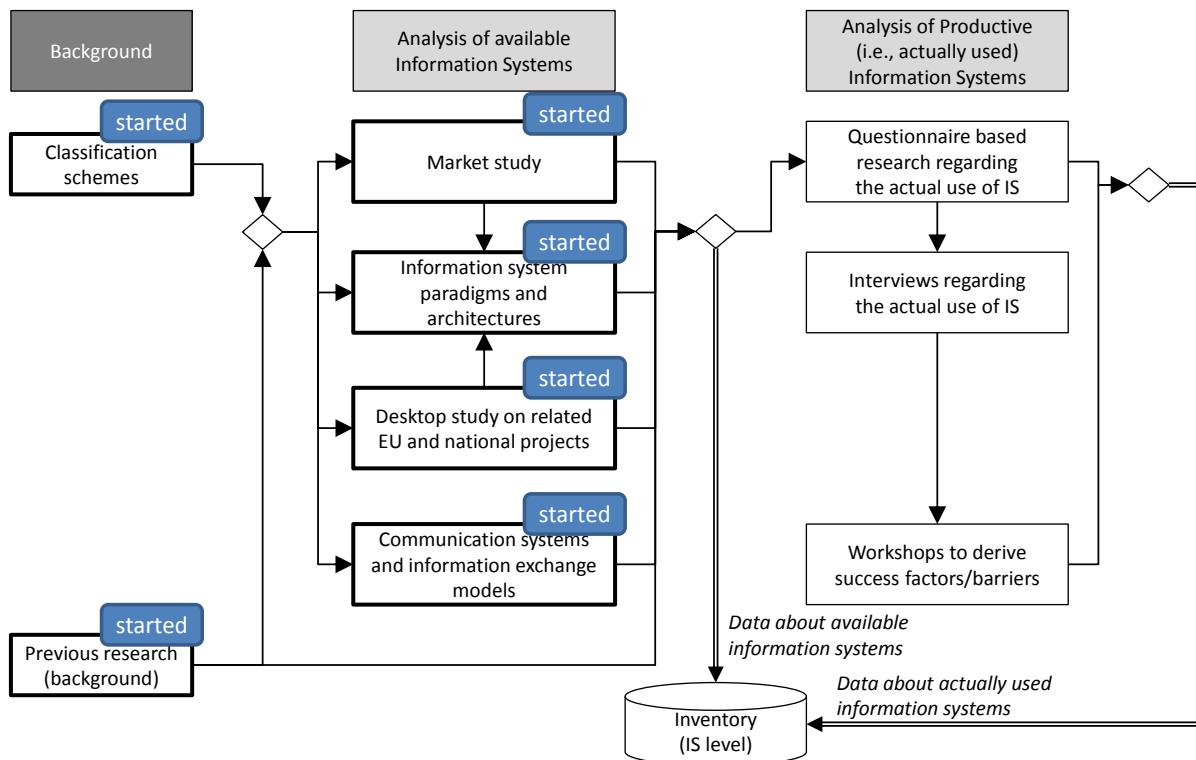


Figure 16 Current status of activities in task T3.3



These can be listed as follows:

- Identification of **background** and conduction of **Market** and **Desktop studies** for performing a first study on information systems: As different members of the SecInCoRe consortium are already involved in technical oriented and application based research projects in the domain of public safety and security, results and experience on this basis enables to elaborate a first overview of information systems and to derive a classification scheme for these. In order to extend the overview of information system on basis of SecInCoRe background, 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.
- Research on IS **paradigms** and **architectures**: Another important aspect is the context of information systems lies in the structure of specific applications. Especially for IS providers is important to know which structures offer special advantages and disadvantages. Thus the research on paradigms and architectures is necessary to derive conclusion regarding those issues. To address this, one type of activity was focused on the collection of existing information system paradigm and architectures. Based on these results first analysis were initiated.
- Analysis of **communication systems** and **information exchange models**: Besides the structure of information systems the interfaces to other systems is also important. As this is a major issue within the definition of exchange formats, research in SecInCoRe was performed in this area. This allows the identification of data transfer between different systems. For that purpose also communication systems are important as well. Thus the search and analysis of information exchange formats was complemented by research on respective systems and their characteristics.

4.2 Results of these activities

Though the questionnaire at the BSSAR in Heraklion was intended to address issues in Task T3.1 (see paragraph 2.2.4) an interesting aspect for the research on information systems came up. Through conversation with officers and end-users, these groups became apparent that the information systems used by Hellenic agencies are mostly military systems, details for which were not available to the SecInCoRe consortium. In the search for the system used during data collection from organizations such as the Meteorological agency, it was reported that the system used is this of the military, hence confidential. Thus further activities will be conducted to collect and analyse those systems or respective information.

All in all three activities have been conducted for Task T3.3. To get a first overview of information systems in the field of public safety and security a market analysis has been conducted (see paragraph 4.2.1). A survey on software design paradigms and architectures allows a perspective of the technological groundings of information systems (cp. Sub-Section 4.2.2). These activities were complemented by a look at communication systems and data exchange models in paragraph 4.2.3.



4.2.1 First survey on information systems

In the previous deliverable D3.1 of WP3 all descriptions are based on the definition of information management according to Krcmar. In his book (cp. [Krcm05]) he describes information systems as follows: “*socio-technical (‘human-machine-’) systems, which include human and mechanical components (subsystems) and sub-serve the main goal of providing information and communication in an optimal way under economic criteria*” (Translation of [Krcm05, p. 25]). Krcmar defines four major aspects for the optimal provision of information and communication

- provision of concrete and up-to-date information and knowledge
- on the right time and location
- in an appropriate way
- to an eligible group of persons (cp. [Koc13, p. 20V4])

These main aspects are used for a first market analysis regarding information systems in order to reduce the scope of the survey. For a first approach the scope of the market study is further limited as the initial focus is on systems used for the management of crisis. Thereby the term management includes the Tasks planning, organization, lead and monitoring. A crisis represents here an “*exceptional emergency situation, which asks for decisions which haven’t been made before*” (Translation of [Sch07. p. 322]).

The result of the survey is a catalogue describing different systems addressing the issue mentioned here. In order to compare information systems with each other several characteristics for the description of them were defined. These are oriented on the following questions:

- What’s the name of the system and from whom can it be purchased?
- Which organisations are addressed as end-user?
- What are the special features of the system?
- What areas are covered by the system?
- In which language is the system available?
- How can other systems be connected to the information system?
- Which options for communication does the system provide?
- Which hardware is needed for the system?

In order to address those questions eight modules were considered (see Figure 17).

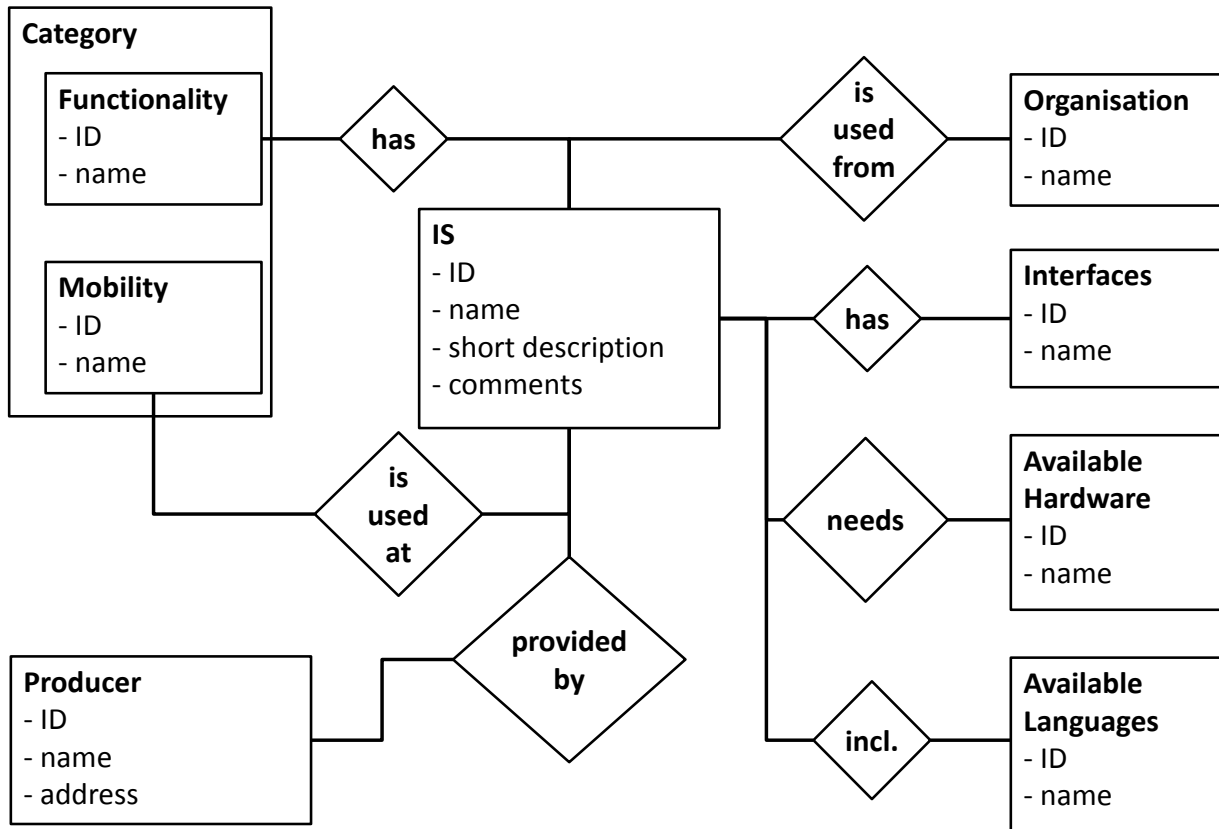


Figure 17 Database scheme for information systems

Most of the modules are quite comprehensible (title, short description, etc.) but there are few which need to be described. The object “Category” gives a tabular overview which functionalities (e.g., GIS, Communication/Alerting) are provided / considered by the regarded system (row) and where (Control room, mobile APP, etc.) the system can be used (column). As some functionalities are sub-categories of others (e.g., GIS navigation of GIS) multiple entries can be done here.

The module *Organisation* provides an overview of the system’s main user groups. According to the focus on information systems for crisis management user are categorized in *Fire department, Police, Emergency services, Technical Emergency Relief, Military, Security services* and *Aid organisations*. As there are many other authorities and organisations with security Tasks there is also a box *Others*.

The module *interfaces* describes the communication potentials of the information system to other systems or hardware respectively. Thereby many different kinds of interfaces are considered (i.e., GPS as an exchange format and telephone, fax or pager as hardware type, which allows the derivation of formats like SMS and Email).

The box *Available Hardware* includes a description of hardware on which the information system can be installed and processed. These are normally divided in PCs, smartphones and tablets. The module *Available Languages* lists the different language versions of the information systems. In the box *Producer* provides name and contact data of the information system’s manufacturer. The last module *Comments* allows to add characteristics and further information regarding the information system.



In the following a template for the information system “*Euro DMS*” is presented describing the components of the database (equivalent to the characteristics of every information system) in more detail:

Euro DMS

Short description:

The producer Euro DMS (Disaster Management System) provide a modular solution for the formation of an individual control station system. Available modules are disposition, documentation, messaging, resource management, persons affected, operational picture, and public relation work. The module *disposition* allows integration of current operations and individual resource dispositions in a complex overall map. For this purpose different analogue and digital alerting procedures and radio communication analysis can be conducted. Moreover this module enables the direct transfer of operational orders to operational units via satellite-based navigation devices. The component *Documentation* supports the protocolling and documenting of operations parallel to its response. One special feature is the finalisation of documentation at the end of an operation, which disables the post-processing of the documentation and ensures work in legal framework. The module *Message* is the information and communication system component. It replaces the manual fourfold forms (in German: “*Vierfachvordruck*”) and extend communication with Email and Fax. Compared to conventional fourfold forms it includes features like optical and acoustic signals, automatic prioritisation and remember capabilities. The functionality *operation management* enables the coordination of operational units during the response to an incident. It supports disposition and monitoring of units as well as the preplanning of upcoming operations. Another module is called *Victims* which includes the tracking of persons affected. One special characteristic is the identification of person descriptions according to biometric data. The GIS module from the company Euro DMS is the *operational picture* component. It allows creating and adapting operational pictures, getting an overview about the incident scene and locating units and vehicles via GPS. The component *public relations* supports subject area S5 in the operational command according to the FwDV100 and thus enables the automatic informing of public media about the current status.



Category:		Control room	Mobile control room	Vehicle	App	Others*	
	GIS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	(GIS) Navigation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	(GIS) interactive Map	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	(GIS) Tracking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Operation planning and Operation monitoring	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Communication / Alerting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Resource and vehicle Operational unit disposition	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Databases	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Logging	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Archiving	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	Others**					<input checked="" type="checkbox"/>	
	* Operation centre						
	** Public relations						
	Organisations:						
Fire department <input checked="" type="checkbox"/>							
Emergency services <input checked="" type="checkbox"/>							
Police <input checked="" type="checkbox"/>							
Technical emergency relief <input checked="" type="checkbox"/>							
Military <input type="checkbox"/>							
Security services <input type="checkbox"/>							
Aid services <input checked="" type="checkbox"/>							
Others <input type="checkbox"/>							
Interfaces:							
- Analogue & digital radio							
- Fax							
- Email							
- GPS							
- SMS/telephone							
Available hardware:							
- PC							
Available languages:							
- German							
Producer:							
Euro DMS							
69 Great Hampton Street							
UK-B18 6 EW Birmingham							
West Midlands							
Company No. 5449784							
www.euro-dms.de							
Comments:							

Figure 18 Characteristics of an IS illustrated exemplary on Euro DMS

The first survey was based on literature and a web based research. Thereby more than 60 systems were gathered and described according to the template (see Figure 18). Thus those systems can be included in the database when implemented:

4.2.2 Information system paradigms and corresponding architectures

Due to the nature of the research item here, the following descriptions are very technical and are mainly addressed for readers, who are quite known in the area of programming.

According to the “Oxford Dictionary” one meaning of *paradigm* is “a typical example or pattern of something; a pattern or model” [Stev10]. The term paradigm in the scientific context can be attributed to Thomas Kuhn and his book “The Structure of Scientific

Revolutions” (see [Kuhn62]). In the “*Oxford Dictionary of Philosophy*” this is described as follows:

“Kuhn suggests that certain scientific works, such as Newton's ‘*Principia*’ or John Dalton's ‘*New System of Chemical Philosophy*’ (1808), provide an open-ended resource: a framework of concepts, results, and procedures within which subsequent work is structured. Normal science proceeds within such a framework or paradigm. A paradigm does not impose a rigid or mechanical approach, but can be taken more or less creatively and flexibly. [...] A paradigm is only upset in periods of revolutionary science, typically arising in response to an accumulation of anomalies and stresses that cannot be resolved within its framework.” [Blac08]

Stephen H. Kaisler utilises in [Kais05] this idea of paradigm for the analysis of programming languages as well as software architectures in order to determine how several types of problems are solvable. The author introduces a hierarchy of structural paradigms based on different levels of abstraction (see Figure 19).

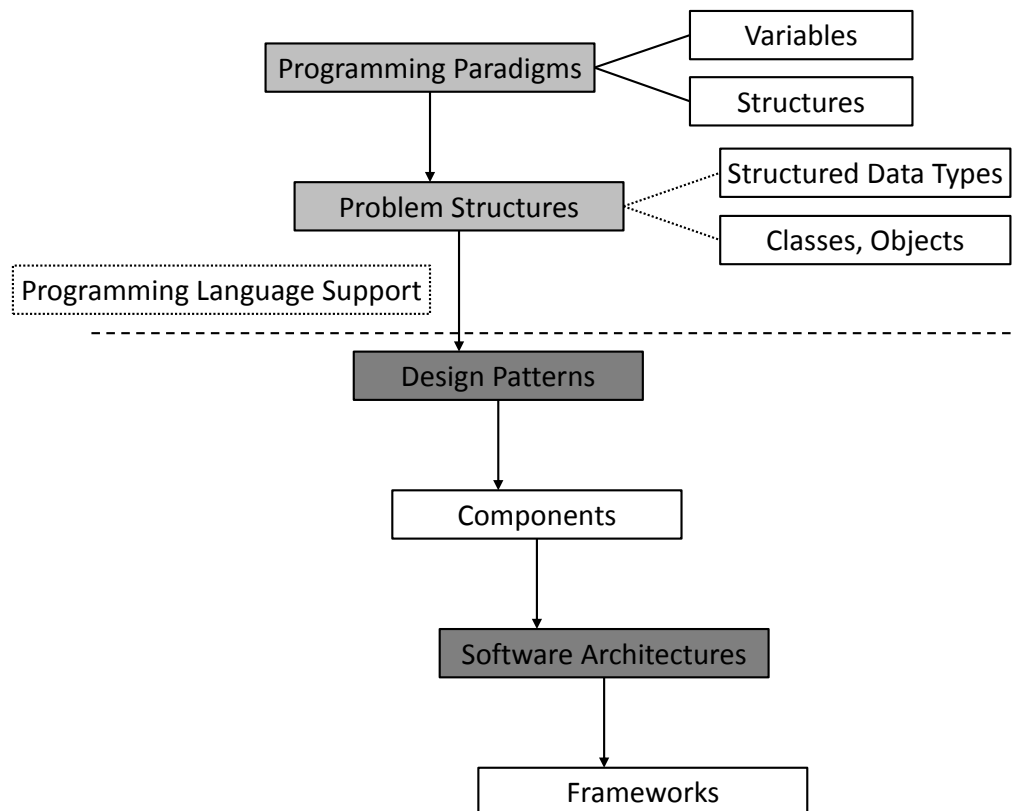


Figure 19 Hierarchy of structural paradigms acc. to Kaisler
(Source: [Kais05, p. 12])

Programming paradigm (i.e., imperative or object oriented) as well as problem paradigm (for example to solve sequential or concurrent problems) are on very detailed levels requiring much knowledge about the fundamentals of programming. Thus this deliverable targets more abstract issues and considers design patterns, components, software architectures and frameworks.

Design patterns are according to Kaisler “a proven solution for a general design problem. It consists of communicating objects that are customized to solve the



problem in particular context. The usefulness of the solution a pattern represents has been proved in many designs. As such, it captures the design experience of experienced programmers.” [Kais05, p. 28f.]

Thus design patterns help designers to solve problems in an efficient way without developing a new design completely. Usually in technical context they are models of partial solutions and connected with object oriented programming, though they may be used in programs based on other programming paradigm. Kaisler points out, that a pattern has to be instantiated - the programmer has to write code and to make decision of how operations should be conducted. In this process patterns can be used for support but the functionality has still to be written. (cp. [Kais05, p. 39])

In 1995 the Gang of Four (GoF) listed 23 different patterns (cp. [GHJV95]). These are divided in three categories of design patterns depending on their purpose: *“Creational patterns concern the process of object creation. Structural patterns deal with the composition of classes and objects. Behavioral patterns characterize the way in which classes or objects interact and distribute responsibility.”* [GHJV95, p. 10] On this basis other patterns have been derived, e.g., by [Schm96] and [Lea96]. An example for a creational pattern is *“Singleton”* as one of the *“most-cited design patterns that were included in the GoF book. Sometimes it is necessary, and often sufficient, to create a single instance of a given class or object. Restricting the number of instances may be necessary or desirable for technological or business reasons, such as a GUI application must have a single mouse [...]. The Singleton pattern applies to the many situations in which there needs to be a single instance of a class - a single object.”* [Kais05, p. 49f.] According to [GHJV95, p. 127] the singleton pattern enables a class having only one easily accessible instance by making the class itself responsible for granting an unique instance. The structure of the Singleton pattern is illustrated by its UML representation in Figure 20.

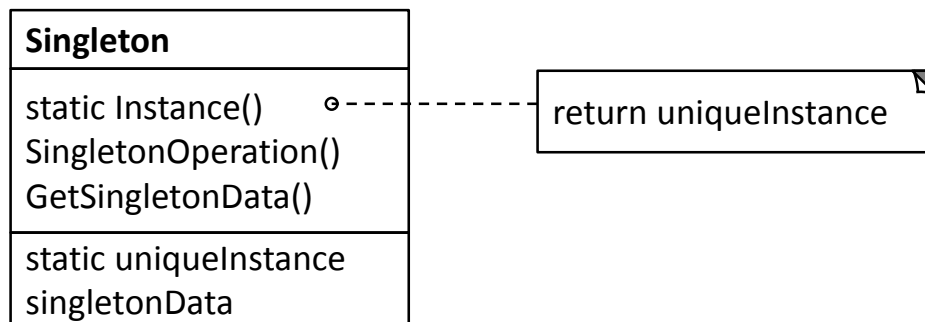


Figure 20 Singleton pattern
Source: [GHJV95, p. 127]

Other creational patterns are *“Builder”* and *“Factory Method”*, while structural patterns are *“Bridge”* and *“Composite”*. Two examples for behavioural patterns are *“Mediator”* and *“Observer”*.

Patterns as abstract concepts for solving problems are instantiated by components (see Figure 19 on page 44). This means that components are specific implementations of these abstract concepts. Kaisler understands *“component software as an object-based software model aimed at efficient and incremental software development. The main idea is to break monolithic applications into reusable, binary components that can be developed, distributed, and upgraded independently.”* [Kaisl05, p. 30]

Since problems which shall be solved by software get larger and more complex this also counts for respective information systems (cp. [Kais05, p. 197]). As a consequence these systems are not developed to solve single problems but to solve classes of problems - so called *problem spaces*. *Software architectures* describe the structures of components solving a problem space. Therefore the problem space has to be disassembled into small pieces with common properties and solutions for each of these - components - have to be found. The single components have then to be integrated and made interoperating so that the result is a piece of software or application for solving the initial problem. The integration describes a well-defined composition of those pieces (ensuring physical communication), interoperation an efficient collaboration (ensuring logical communication) which produces an answer. (cp. [Kais05, p. 3ff.]) In accordance with Garlan “*software architecture typically plays a key role as a bridge between requirements and implementation*” [Garl00, p. 94]. A architecture comprises different elements (see Figure 21). The basic building blocks as active computational entities are components with properties - so called *attributes*. Components communicate via one ore multiple *interfaces* with their environment including other components. A *connector* interlinks interfaces of two or more components and describes so the interaction between those and respective rules within. Attributes appended to the connector define the behaviour of the regarded components. A *configuration* (or topology) describes the architectural structure as a connected graph including components and connectors.

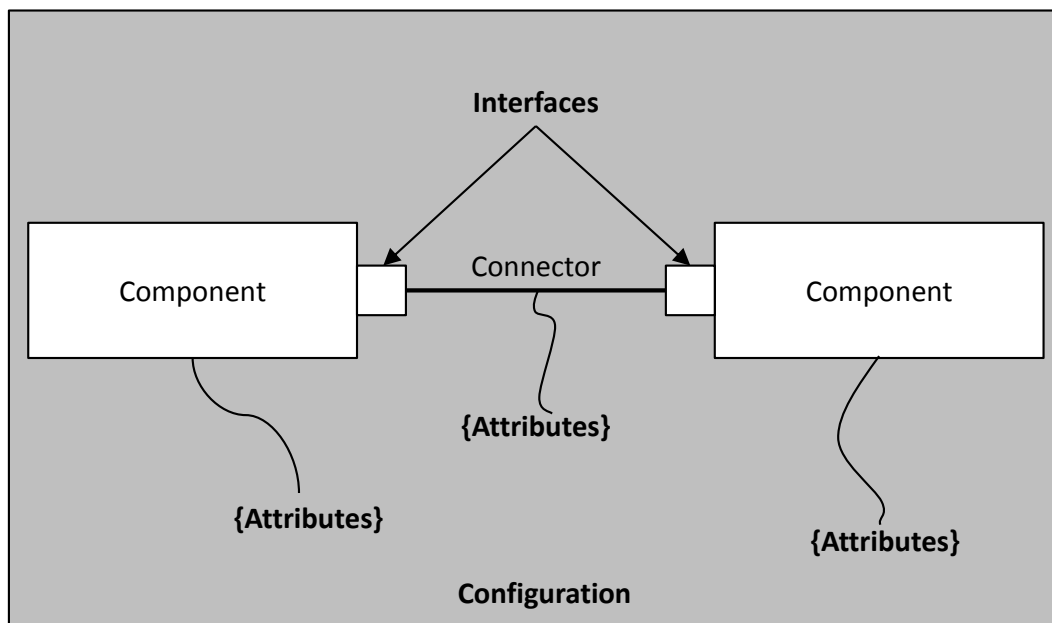


Figure 21 Software architecture concept

Source: [Kais05, p. 200]

Architectural paradigms define the kind of apprehending computing systems (e.g., design and configuration) as the collocation of hard- and software as well as of telecommunication units. A simple association of components does not result in a solution. A topology describing their interaction and communication as architectural style has to be introduced to guarantee integration and interoperation. As some architectural structures repeat themselves the introduction of patterns is most reasonable here. On this basis there exist many different software architectures. An



early example of the late 1980s is the “*Domain-Specific Software Architecture (DSSA)*” (cp. [Kais05, p. 208ff.]. Thereby a domain describes a field of interest, normally as representation of a problem space. The DSSA program targets a practical reuse of software through the development of component-based solutions for problem domains. Since the components are generic they have to be tailored while implementing a specific application.

Garlan and Shaw describe different architectural idioms corresponding to specific architectural styles (see Figure 22). They list five different architectural styles and refer several idioms to these. The idioms can be divided in different architectures. For instance the “*Distributed Feature Composition*” (see [JaZa98]) and the “*Unix Shell*” (see [GaSh94]) are examples for pipes and filter architectures. Kaisler assess the different architectural styles with regard to specific criteria like extensibility or flexibility (see [Kais05, p. 328ff.]. These aspects will be analysed in the further progress of SecInCoRe as well to derive recommendations regarding specific architectural styles, idioms or specific architectures.

Architectural Style	Architectural Idiom
Data flow systems	Batch sequential
	Pipes and filters
Call-and-return systems	Main program and sub-routines
	Client-server systems
	Object-oriented systems
	Hierarchical layers
Virtual machines	Interpreters
	Rule-based systems
Independent components	Communicating processes
	Event-based systems
Data-centred systems	Database systems
	Blackboard

Figure 22 Classification of architectural styles
Source: [Kais05, p. 219] according to [GaSh94]

In Figure 23 there are also *Frameworks* illustrated. These are closely related to design patterns as well as components. Kaisler describes them as follows: A “*software*

framework is a reusable mini-architecture that provides the generic structure and behavior for a family of software abstractions, along with a context of metaphors that specifies their collaboration and use within a given domain. [...] A framework is usually not a complete application: it often lacks the necessary application-specific functionality, although it may include considerable domain knowledge embedded in its definition. [...] Thus, a framework supplies the infrastructure and mechanism that execute a policy for interaction between abstract components with open implementations.” [Kais05, p. 35] A framework supports the pre-definition and pre-implementation of difficult parts of the solution in the problem domain.

There exist different types of frameworks and respective classification schemes. Fayad and Schmidt developed two classifications for example. The first of these regards the structure and the scope of the framework and divides into “System Infrastructure Frameworks”, “Middleware Frameworks” and “Enterprise Application Frameworks” (see [FaSc97, p. 34f.]). The other categorisation of frameworks has the focus on the usage of frameworks and includes “White-Box Frameworks”, “Black-Box Frameworks” and “Grey-Box Frameworks” (see [FaSc97, p. 35]). For the construction of a framework layered framework architectures can be utilized. Kaisler describes the several elements of these and illustrates them according to Figure 23.

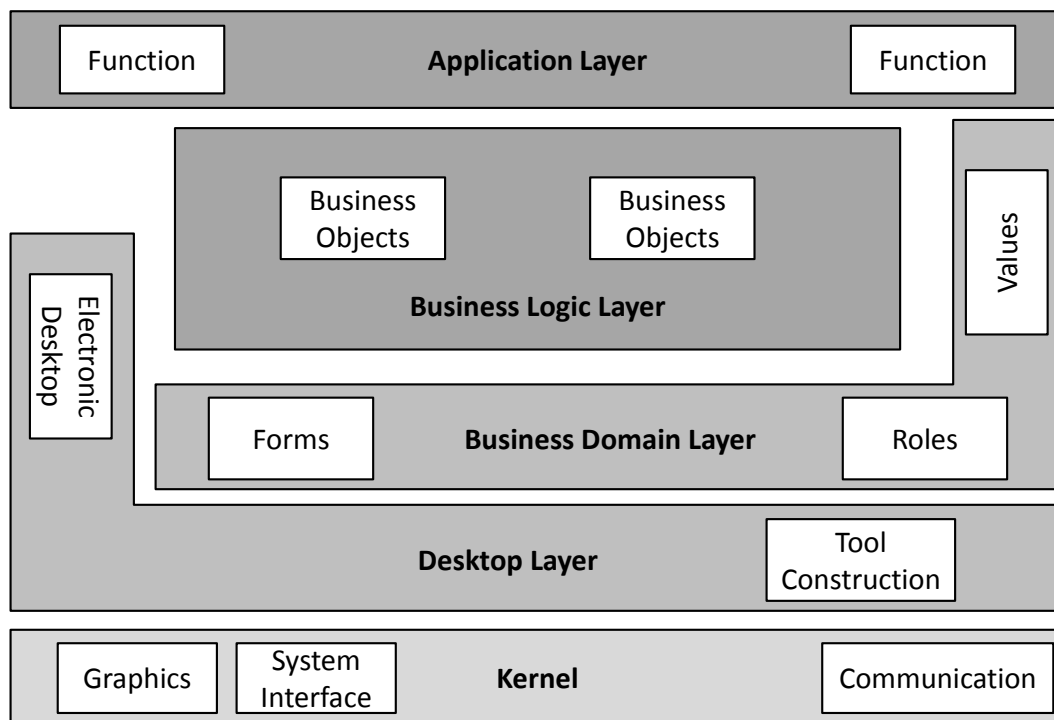


Figure 23 Layered framework architecture
Source: [Kais05, p. 351]

The coherences between design patterns, components, architectural models and frameworks and their dependencies with information as well as communication system in the domain of public safety and security will be further analysed in SecInCoRe. The relationships described here help to understand different approaches for structuring software and allocate categories of software models. In the ongoing process of SecInCoRe it will be used to derive top-down a general structure for information and communication systems in the field of public safety and security. This approach will be



complemented by a bottom-up analysis on architectures of specific information and communication systems utilized in the area of public safety. For this purpose a first survey has been conducted. Thereby publications and figures regarding concrete architectures of the following systems were gathered:

Information / Communication System	Description of architecture
ABSOLUTE	see [www3]
Airborne Base Stations	see [ARG+13]
ArcGIS	see [WrYo06]
BAYSAT-KRISIS	see [SiBa11]
BRIDGE	see [Zimm13]
CLIMB	see [BGD13]
COPE	see [www4]
DISASTER	see [CaRu13]
EULER	see [SCA+09]
FireSim	see [Schm10]
FREESIC	see [MLV13]
LIMES	see [WGG+10]
metropoly BOS	see [LSN14]
NICOLE	see [GTD+12]

Figure 24 Excerpt of list regarding Information / Communication Systems and their architecture descriptions

The results are utilised to identify specific structure patterns. Both actions will result in a list of architecture patterns and respective systems.

Besides information systems and their architectures, communication systems are quite important for SecInCoRe. Thus some of these as well as data exchange models enabling communication between information systems are analysed.

4.2.3 Communication systems and information exchange models

The survey of information systems was complemented by an analysis on communication systems. These are described in short according to categories



described in the following. It is to mention that the main focus of Task T3.3 is on information systems. Thus communication systems will not be analysed in the same detail level as information systems (see Section 40). Besides the *Name* and a *Short description* the characterisation of communication systems comprises a *Link* to a respective webpage as well as naming of the *Producer*. An excerpt of the list is described in Figure 25.

Communication System	Short description	Link	Producer
A4A (Alert 4 All)	Alert and communication towards the population in crises management	http://www.alert4all.eu/	European Commission (Belgium)
ABSOLUTE (Aerial Base Stations with Opportunistic Links for Unexpected & Temporary Events)	A rapidly deployable multi-purpose, multi service and multi-band interoperable and integrated network infrastructure capable of supporting reliable high data rate applications to serve large scale disaster emergency situations and the temporary event scenarios.	http://www.dlr.de/kn/desktopdefault.aspx/tabid-2081/6933_read-37709	DLR Institut für Kommunikation und Navigation (Germany)
ACM (Adaptive Coding and Modulation Modem for Broadband Communication)	Demonstrator to test techniques for adaptive coding and modulation in broadband satellite systems	http://www.dlr.de/kn/desktopdefault.aspx/tabid-4309/3222_read-4701/admin-1/	DLR Institut für Kommunikation und Navigation (Germany)

Figure 25 Excerpt of the list regarding communication systems

The complete list shows that there is much research in the area of communication systems. Based on the background knowledge of the consortium members there are only two different producers (DLR and EC) considered. In the further progress of this research communication systems of other providers will be regarded as well.

Besides communication systems, data or information exchange models are collected and analysed to research on communication of information systems. Since a coherent data model for data exchange is indispensable for enabling interoperability in emergency management there exist various information exchange models for



emergency situations. One of them is the *EDXL*²⁰ (Emergency Data eXchange Language) which is mainly used in the United States (see [GuDw10]). EDXL is divided in four layers, which handle:

- the routing of the raw data
- connection of the different systems
- routing of the needed information to the stakeholders with EDXL-DE
- transportation of information in different standards supported by the system

An example for a specific EDXL format is CAP (Common Alerting Protocol) which “provides an open, non-proprietary digital message format for all types of alerts and notifications. [...] The CAP format is compatible with emerging techniques, such as Web services, as well as existing formats.” [www6]. The main use of CAP lies in the activation of all alerting and warning systems on the basis of single input. Moreover, it enables the normalization of warnings from several sources in order to condense and match them for enhancing situational awareness.

Besides the aforementioned models there is the TSO (Tactical Situation Object). This language enables the exchange of information during an operation. The TSO is a definition of information structure for recording a view on a situation from a particular observer at a specific time (see [www5]). Thus, it can be used to provide this view to other observer. In this context an observer can represent several things. It ranges from a simple machine like a transponder to a complex IT-system like for command and control. It is interoperable with the EDXL-DE format but does not enable free text descriptions. Moreover it does not consider the merging of different messages.

Another exchange model is the *PRML* (Protection and Rescue Mark-up Language) that was developed in the SPIDER project²¹ in Germany (see [SRWW10]). It is characterised by an extreme heterogeneous system environment due to several civil protection organisations without federal command structure. PRML aims to be a common data model for the interaction of concerned components and tries to include all necessary elements. In comparison to the EDXL-Model the main difference are the lower overhead, caused by the stake-holders choice of providing and requesting various data (see Figure 26). The system links the different sources to different entities and only provides what is really needed to know without additional overhead. So the information flood is reduced to a minimum.

EDXL	PRML
Neutral data model	Specific data model
Exchange of announcements	Combination of data source
No implementation of gateways	Gateways part of the specification

²⁰ For more information take look on the Oasis Homepage (www.oasis-open.org).

²¹ For more information take look on the SPIDER Homepage (www.spider-federation.org).



EDXL	PRML
Filtering possible, but not standardized	Explicit filtering of Data intended

Figure 26 EDXL and PRML in comparison

Another German example is the exchange model DIN SPEC 91287 (2012), Data interchange between information systems in civil hazard prevention, developed in the project LAGE²² based on a more detailed approach called xHelp (see [LHPK10]) that enables the information transmission independently from the channel (e.g., usage of a USB stick, Internet based transmission) based on XML. This enables the interoperability between different IT-based control systems in semantical, technical and organizational issues.

In Germany, the Federal Office of Civil Protection and Disaster Assistance (BBK) pushes another standardisation initiative to describe the types of data sets that the authority is responsible for. The standard is call “xKatastrophenhilfe” (English: xDisastermanagement)²³, it is based on the XÖV framework (established by the German coordination authority for IT standards)²⁴. SecInCoRe intends to establish a close cooperation with the BBK for further research (see creation of the Advisory Board described in [15]).

In the further process of SecInCoRe these models will be analysed in more detail, e.g., regarding their deployment in practice. Additionally other data and information exchange models will be researched in order to derive important characteristics as well as necessary elements.

²² For more information take look on the LAGE Homepage (www.lage-projekt.de)

²³ <https://www.xrepository.de/Inhalt/urn:uuid:08f6f5fb-e28f-49c5-bf95-c65b81db881c.xhtml>

²⁴ <http://www.xoev.de/sixcms/detail.php?gsid=bremen02.c.730.de>

5 Business models for the application of information systems

One major aspect of SecInCoRe is the research on existing business models and the derivation of new crisis management models including also business relevant aspects (cp. [3]). A first description of relevant issues in the area of business models in emergency management was made in the first deliverable of this work package (see [5]). Thereby two foci were defined which are the basis for activities in this area:

- Procurement (e.g., of data sets, information systems)
- Public-private partnerships (PPPs)

The correlation between these both aspects is described in more detail in [5].

5.1 Activities for analysing business models

According to the research framework the research regarding business models is initiated by analysis of regarding law, procurement directives and guidelines. Due to the actual activities in this work packages one deviation has been made: Since many efforts in SecInCoRe have been already undertaken to collect and analyse information system (see chapter 4), first activities in the area of analysing business models were focused on the procurement of information systems (cp. Figure 27).

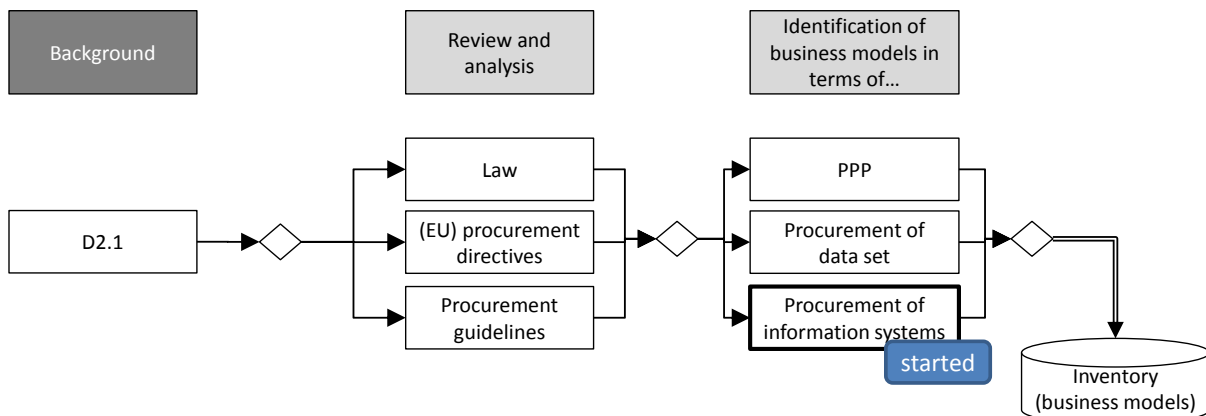


Figure 27 First activities for analysing business models

For analysing the **procurement of information systems**, a literature analysis has been conducted. All activities were focussed on procurement models and their characteristics. In the further process, more guidelines, regulations, and descriptions of procurement processes and procedures will be researched on. Thus, an overall picture about current approaches will be gained and best practices as well as lessons learnt will be derived.

5.2 Analysis of business models for the application of information systems

First responders and Police authorities do rely heavily in information system and telecommunication infrastructure access and sharing. Those systems and infrastructures are often shared among agencies, like the telecommunication infrastructure, while others are managed and operated by each agency for its own needs. Agencies are continually challenged to provide excellent quality of service in the face of increasing threats and changing needs, indeed governments are looking for



ways to provide consistent, improved quality of service at predictable costs and to adopt new technologies with lower upfront investment²⁵.

Moreover those infrastructures are linked to more complex infrastructure based on diverse technologies, vendors and domains, and adding to this, most public safety emergency service personnel, system administration and telecom management is not their core mission — which adds to the challenge of operating and managing those networks and information systems²⁶

To implement new system and to interoperate with others public safety network without disrupting existing day-to-day operations, public safety agencies must consider a number of key issues, including multivendor interoperability, network reliability, scalability and interworking.

Approaching the way in which systems are improved or extended each agency takes into account the following considerations:

- Optimizing the total cost of ownership (TCO) of the systems
- Selecting the correct technological solution
- Minimizing implementation and technical risk
- Securing migration from present mode of operation (PMO) to future mode of operation (FMO)
- Setting up network operations efficiently to reduce OPEX

In a traditional model agencies would have followed one of the following models

- *CAPEX model*: All equipment and software is purchased, and ongoing support is provided through in-house personnel.
- *Managed model*: All equipment and software is purchased, but the ongoing support is either wholly provided by another party, or the support is shared by another party and in-house personnel.
- *Hosted model*: Network access is provided by another party and leased to a public safety entity for a monthly fee.

The Capex Model²⁷

In the CAPEX model, the overall network and information system is owned and managed by one or more First responders and Police authorities. These entities take full responsibility for purchasing all network elements and software, and they employ in-house personnel to build, manage, operate and maintain the network. Being critical systems they are normally built with complete geographic redundancy to eliminate

²⁵ Chen, Rui; Sharman, Raj; Chakravarti, Nirupama; Rao, H. Raghav; and Upadhyaya, Shambhu J. (2008) "Emergency Response Information System Interoperability: Development of Chemical Incident Response Data Model," Journal of the Association for Information Systems: Vol. 9: Iss. 3, Article 7.

²⁶ Approaches to Statewide Collaboration and Information Sharing, HomeLand Security US Government

²⁷ PROSIMOS Priority Communications for Critical Situations on Mobile Priority Communications for Critical Situations on Mobile D1.3



single point of failure. This approach, while guarantees dependability, increases costs for core network and system equipment, beyond what is usually required for commercial networks. Initial upfront costs can be offset — and ongoing OPEX costs can be reduced — through government grants and incentives, along with any reallocated fees (which may currently be paid to commercial broadband wireless and wired service providers). The extent of upfront costs depends on: the scale of deployment (local or regional), whether the core network is shared among multiple areas or entities and how deployment is scheduled (gradually over years or within a shorter time period). With the CAPEX model, the First responders and Police authority entities must also employ skilled personnel for network design, operations, maintenance, security and technical support, as well as program and project management. The CAPEX model can be a good option for public safety entities that deploy their own network as long as they have “critical size.” Critical size is determined by comparing the total allocated costs with the cost of an equivalent outsourced or managed service.

Managed model

The managed model is a hybrid, combining elements of the CAPEX and hosted models. With the managed model, the First responders and Police authorities is responsible for ensuring that network information systems elements are appropriately owned and deployed. But it contracts with another party to manage and/or operate the network and/or part of the system.

Similar to the CAPEX model, this model requires each public safety entity to purchase all the equipment and software and contract for the required deployment services. Depending on the network architecture, these costs can vary significantly. Though in this model, cost savings are possible by contracting management functions with another party. For the highest Quality of Service (QoS), management services should go beyond traditional network and system and provide a performance management platform that proactively monitors for predetermined thresholds, along with preventive maintenance to ensure all system elements are running at peak efficiency. In doing so, the network is managed proactively to maintain network availability while ensuring a high degree of service uptime.

The managed model offers flexibility in terms of the management functions contracted. For example, a public safety entity could have another party provide end-to-end operational support, using a service-centric approach. This approach provides operational support from the core through the network to the end user.

The managed model provides a degree of control to each First responders and Police authorities entity. Owning the assets allows each public safety entity to decide when to upgrade the network and implement its own security platform. By contracting with another party to provide management services, the public safety entity will have a predictable monthly fee with lower IT and administrative headcount. It will also require less investment in network management tools and training.



Hosted model

The hosted model allows each First responders and Police authorities to use network assets that are owned and managed by another party. These assets are usually shared among several similar types of customers with similar needs, creating economies of scale for both capital and operational expenses. While core infrastructure is shared, tele-communications are usually owned — and may be unique to — each individual First responders and Police authority entities. The shared core provides the benefits of the platform while reducing start-up costs and ongoing operations costs. With a hosted model, the public safety entity pays a consistent, predictable periodic fee for network access and system use. The fee is usually a function of some known factor, such as the number of users, usage, service agreements etc.. This model also eliminates the need to plan and allocate funding for network upgrades, maintenance contracts and ongoing training for operations. These expenses are all handled by the hosting provider, who is responsible for keeping the platform current, resolving all technical issues and ensuring the appropriate level of service.

The figure shows the cost profiles for the three deployment options. Start-up costs are greatest for the CAPEX model, because it requires equipment purchases, software licensing, employees and training, management tools, facilities and circuits. The managed model also requires initial capital purchases, but headcount and training needs are lower. Start-up costs for the hosted model are substantially lower.

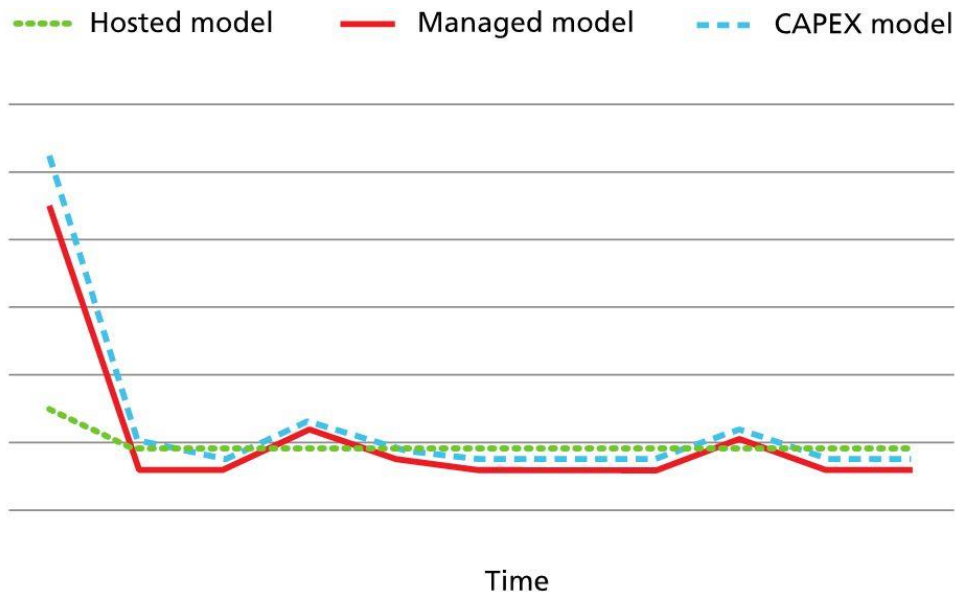


Figure 28 Cost Dynamics

Over time, the CAPEX and managed models may have a periodic lower cost, but they will see spikes as upgrades and training are incurred, and as the platforms are kept up to date. After initial start-up, the hosted model will provide a consistent, known cost. To determine which model provides the best financial view, a full lifecycle analysis needs to be completed. For the CAPEX and managed models, a number of assumptions would be required, while the hosted model has known costs for comparison. Aside from costs, each model has its own pluses and minuses, based on each public safety entity's individual needs, resources and capabilities.



- The CAPEX model provides the greatest level of internal control but also requires the highest funding and skilled headcount.
- The managed model helps to level out ongoing operational costs but still requires a significant initial capital outlay.
- The hosted model provides the most predictability — helping each public safety entity manage and control costs, while offering a platform that will stay more up to date than a locally deployed infrastructure. However, it does require public safety entities to be comfortable with a greater amount of third-party control.

With both the managed and hosted models, degrees of control can be shared between the public safety entities and the service provider. While complete control and operations can be contracted, public safety entities can also maintain a level of management they are comfortable with and have the resources to support. This shared control could be as simple as setting up alarm conditions that both parties can see. Or it could be more operational, allowing public safety entities to manage end-user devices for additions, changes and deletions. With a managed or hosted service, public safety entities do not have to give up total control. Mechanisms and processes can be implemented to address any concerns regarding security or control.

The choice of model can only be made after considering the benefits and considerations of each option. But they all require a trusted partner with highly qualified personnel, fully defined support processes, experience in the types of services required and a well-defined security posture. Figure 29 details the aspects to consider. The end result must meet the needs of the departments, municipalities and residences being served.

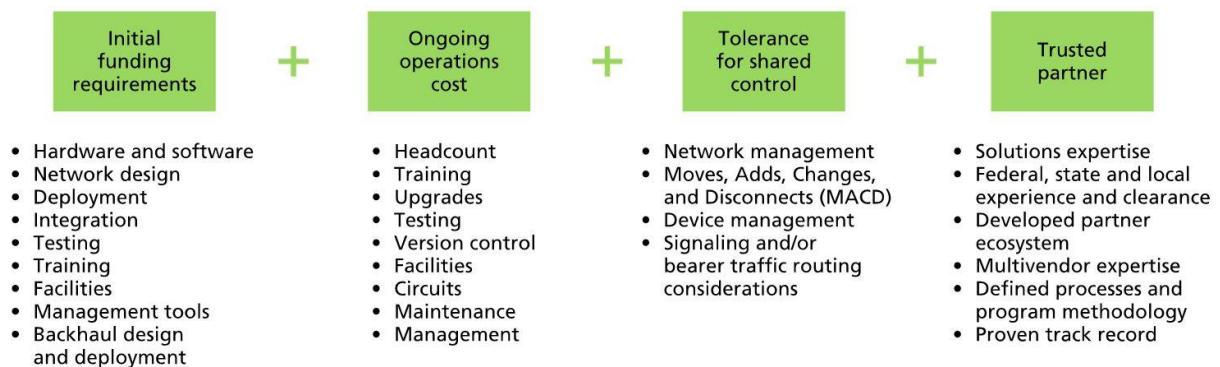


Figure 29 Business Model Evaluation

Cloud Based Model or PSaaS (Public Safety as a Service)

To meet new demand, public safety agencies and technology providers are changing the way their technology is delivered and accessed building multi-tenant Cloud-based application. Public safety and security agencies are moving from a traditional model that requires agencies to purchase, host and manage expensive software and hardware products to the Public Safety as a Service, or PSaaS model²⁸.

²⁸ PSaaS: THE NEXT EVOLUTION OF PUBLIC SAFETY, Tiburon Inc.



It's now clear that moving to the Cloud has several advantages for both public safety technology providers as well as public safety agencies. The elasticity offered by the Cloud can be leveraged to instantly provision resources and on-board new customers quickly. Resources can be pooled to create new applications that require intensive computing power. The Cloud enables storage of vast amounts of data that can be correlated and aggregated into intelligence, which can be shared by public safety agencies.

The Cloud delivery model facilitates the Software as a Service business model, with little upfront investment required by customers. Public safety agencies can subscribe only to services they need and yet have access to cutting edge technology. Since there is a single point of management, new product features become available instantly to all agencies across the board. This delivery model helps agencies increase efficiency and keep operational costs under control. Moreover PSaaS is a major advance for public safety and security as based an open communications protocol, based on the principles of service oriented architecture and proven data exchange formats, allows any standards- based systems to integrate easily, securely and reliably.

While moving to the Cloud provides cost and operational benefits, public safety agencies should carefully evaluate Cloud-based applications they would like to use and technology providers for partnerships. Agencies create confidential records and communications in their day-to-day handling of incidents that are restricted from public access. Moreover, agencies access confidential information from federal and state agencies that require strict controls on who has access to this information and how it must be used and protected. Services offered over the Internet are also prone to availability issues in case of outages.

To evaluate the advantages of PSaaS and its subscription/lease business model, it's important to compare it to the traditional model for purchasing software. In the traditional model, an agency purchases software by paying the vendor a perpetual license fee to use the selected product or products. Fees are typically paid as a large upfront cost that ranges from hundreds of thousands to millions of euro depending on the agency's size and the complexity of its requirements. The license fee does may or may not include annual maintenance and support contracts, which are essential in order to keep the software functioning effectively, and which tend to increase annually. The license to use the software is perpetual, despite the fact that next-generation products inevitably replace all software as platforms, needs and standards change. These large upfront license fees require agencies to raise dedicated capital expense budgets. Obtaining funding of this magnitude typically involves a multi-year acquisition process, spanning political terms and funding cycles, and requiring a significant dedication of time and resources – even before the total cost to purchase and own a solution has been calculated. As a direct result of the difficulty of funding major capital expenses given today's budgets, many agencies with aging systems find it prohibitively expensive to modernize their systems, improve capabilities and meet changing standards via the traditional software purchase model.

PSaaS is based on the understanding that First responders and Police authorities agencies are in the business of protecting people, not managing software, and on the philosophy that agencies should have the option to pay for the usage of software and its capabilities while they use it – not be forced to purchase permanent licenses for



systems that have finite lifespans. PSaaS makes subscription/lease pricing available to agencies that choose hosted or cloud-based deployments as well as to clients that choose to implement software on-site. PSaaS affords agencies several major financial advantages. Up-front acquisition costs for new subscription systems are significantly lower than the upfront costs associated with traditional purchases. For hosted subscriptions, agencies can lower first year costs by up to 60%. For on-site subscriptions, those savings can reach 40%. Since subscription products are often funded out of operating expense budgets, those subscriptions become part of an agency's budget baseline. This means that in times of crisis, there is much less likely to be the same pressure to cut subscription-priced solutions as there would be on capital expenditures, budget increases or new programs. Updates to the latest software releases are included in the subscription fee, allowing agencies to keep their systems current without having to raise additional funds. Lower upfront costs mean that subscriptions can be funded using operating expense budgets over which agencies have much more control, rather than using capital funds, which are significantly more difficult to gain approval for. Subscription pricing is predictable, with the typical 5-year contract specifying consistent annual costs. Subscription pricing typically includes maintenance and upgrades, which can drive more savings. Those agencies that choose a hosted or cloud-based PSaaS deployment rather than installing and supporting the software in their own local data centre can also realise additional cost savings. Indeed Agencies with hosted or cloud-based solutions typically find software updates are installed much more expertly and efficiently since the vendors perform the installation themselves. For on-premises deployments, agencies must plan for peak use and acquire infrastructure accordingly. Hosted and cloud deployments can mitigate the need for agencies to acquire unnecessary hardware, and transfers the expense of software infrastructure (such as SQL licenses) to the provider. Agencies that choose hosted or cloud deployments require fewer of their own IT personnel to perform maintenance and routine technology administration tasks, since the software provider manages the necessary hardware and software. Finally Agencies do not need to deploy security, performance or asset management software to support on-site implementations. Instead, the provider is able to take advantage of significant economies of scale and dedicated resources to provide more sophisticated capabilities more cost effectively.

Public safety and security organizations are constantly being asked to do more work while being provided fewer financial resources with which to do it. Inadequate hardware and software systems are slowing users down. Systems that weren't built to adapt to public safety and security's frequently changing needs are taking up too many resources to maintain and they are expensive to replace. Applications that cannot communicate with each other are preventing agencies from making full use of the data locked inside – data that could help them work more quickly, more safely and more proactively.

Following this brief and initial analysis we can easily understand how SecInCoRe objectives of building a secure, dynamic cloud based knowledge base and communication system concept (including the ability to use emergency information by means of a trans-European communication infrastructure) builds in the direction of the most efficient approach supporting the enabling of a cloud based system for first



responders and police authorities. In general terms speaking of business models in this area might be misleading as system infrastructure cost are bore by government subsidies and only part of the OPEX costs can be shared with providers and operators contracted through public procurement.



6 Literature index

- [ARG+13] A. Valcarce, T. Rasheed, K. Gomez, S. Kandeepan, L. Reynaud, R. Hermenier, A. Munari, M. Mohorcic, M. Smolnikar, I. Bucaille (2013): Airborne Base Stations for Emergency and Temporary Events. In: Proceedings of the 5th International Conference on Personal Satellite Services.
- [BGD13] M. Blaschnek, D. Gerken, R. Duttmann (2013): CLIMB WebGIS-Server and client architecture; final report. Report-deliverable D2.5 of the CLIMB project.
- [Blac08] S. Blackburn (2008): The Oxford Dictionary of Philosophy. Oxford University Press, available at <http://www.oxfordreference.com/view/10.1093/acref/9780199541430.001.0001/acref-9780199541430-e-2303>.
- [CaRu13] R. Casado, E. Rubiera (2013): Reference architecture & data model approach overview – V2. Public deliverable D2.52 of the DISASTER project.
- [FaSc97] M. E. Schmidt, D. C. Schmidt (1997): Object-Oriented Application Frameworks. In: Communications of the ACM, Vol. 40, No. 10, p. 32-38.
- [FPBK09] T. Friberg, J. Pottebaum, B. Birkhäuser, R. Koch, (2009): D6.1.1, Appendix A - Scenario “Emergency Rescue Operation” (ERO). Confidential deliverable, PRONTO - Specific Targeted Research Project im 7. EU-FRP, Grant agreement No. 231738, Paderborn.
- [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.
- [Garl00] D. Garlan (2000): Software architecture: a roadmap. In: Proceedings of the Conference on The Future of Software Engineering 2000, June 04-11, Limerick, Ireland, p. 91-101.
- [GaSh94] D. Garlan, M. Shaw (1994): An Introduction to Software Architecture. CMU-CS-94-166, School of Computer Science, Carnegie-Mellon University, Pittsburgh, PA.
- [GHJV95] E. Gamma, R. Helms, R. Johnson, J. Vlissides (1995): Design patterns, Elements of Reusable Object-Oriented Software. Addison Wesley, Reading, MA.
- [GTD+12] G. Gallinaro, E. Tirrò, F. Di Cecca, M. Migliorelli, N. Gatti, S. Cioni (2012): Next Generation Interactive S-Band Mobile Systems - Challenges and Solutions. In: Proceedings of the 6th Advanced Satellite Multimedia Systems Conference and the 12th Signal Processing for Space Communications Workshop, p. 54-61.
- [ISO11] ISO 22320:2011(E): Societal security — Emergency management — Requirements for incident response.



- [ISO11] ISO 22320:2011(E): Societal security — Emergency management — Requirements for incident response, 2011.
- [JaZa98] M. Jackson, p. Zave (1998): Distributed Feature Composition: A Virtual Architecture for Telecommunication Services. In: IEEE Transactions on Software Engineering, Vol. 24, No. 10, p. 831-847.
- [Kais05] S. H. Kaisler (2005): Software paradigms. John Wiley & Sons.
- [KPJ+12] R. Koch, S. Prödel, A.M. Japs, T. Friberg, C. Lindemann (2012): Mobiles Informationssystem zur Prozessoptimierung in Feuerwehren und öffentlichen Verwaltungen - Mobis Pro (English: Mobile information system for the optimisation of response and preparation processes in fire brigades and municipalities). Final report, Paderborn.
- [Krcm05] H. Krcmar (2005): Informationsmanagement. Springer Verlag, Heidelberg, 4. Auflage.
- [Kuhn62] T. S. Kuhn (1962): The structure of scientific revolutions.
- [Lea96] D. Lea (1996): Concurrent Programming in Java: Design Principles and Patterns. Addison-Wesley, Reading, MA.
- [LSN14] R. Lutz, P. Scheumann, B. Nagel (2014): metropolyBOS - DIE LAGE IM GRIFF. Product brochure of the company GEOBYTE SOFTWARE.
- [LHPK10] C. Lindemann, C. Held, J. Pottebaum, R. Koch (2010): D3 xHelp – Vorschlag zur Standardisierung. (English: xHelp – Confidential project report). Project LAGE, German research programme on civil security, 2010.
- [MLV13] A. Machalek, L. Ladid, S. Vanya (2013): Communication Interoperability in Crises Management. In: InterComms, Issue 21.
- [NN06] N. N. (2006): Major Incident Procedures - What businesses and the voluntary sector need to know. London Prepared - Resilience Through Planning, Camden, available at http://www.camden.gov.uk/ccm/cms-service/stream/asset/414.4%20Major%20Incident%20Procedures%20Leaflet%20A5.pdf?asset_id=2079242
- [PaRa09] G. Patzak, G. Rattay (2009): Projektmanagement: Leitfaden zum Management von Projekten. Linde Verlag, Wien, 5. Auflage.
- [Pott05] J. Pottebaum, (2005): Report on end-user requirements - Final version for the first prototype (D5.1.2), Paderborn. (SHARE - Specific Targeted Research Project im 6. EU-FRP, Contract No. 004218).
- [Pott06] J. Pottebaum, (2006): Final report on end user requirements State of the Art and Release 1 (D5.1.4), Paderborn. (SHARE - Specific Targeted Research Project im 6. EU-FRP, Contract No. 004218).
- [SCA+09] V. Seignole, T. Caderas, M. Ahsant, G. Peliks, A. Kropp, J. D. Ruiz, C. Mathieu, T. Brasy, B. Calvet (2009): System general design. Public deliverable D3.2 of the EULER project.



- [Schm05] D. Schmidt (1996): Asynchronous Completion Token - An Object Behavioral Pattern for Efficient Asynchronous Event Handling. Presented at the 3rd Annual Pattern Languages of Programming Conference in Allerton Park, Illinois, September 2-5.
- [Schm10] N. Schmeisser (2013): A Virtual Firefighting Simulator. In: Proceedings of the International Workshop 'Innovation Information Technologies: Theory and Practice', Dresden, 6.-10.09.2010 , p.75-82.
- [Scho07] H. Scholten (2007): Die Wahrnehmung von Krisenphänomenen: Fallbeispiele von der Antike bis zur Neuzeit. Böhlau Verlag, Köln.
- [SiBa11] T. Sichert, S. Baumann (2011): BAYSAT-KRISIS. In: Satellite Navigation applications in the NEREUS Regions, prepared by the NEREUS GNSS Working Group, p. 11-12.
- [Stev10] A. Stevenson (Eds.) (2010): Oxford Dictionary of English. Oxford University Press, available at http://www.oxfordreference.com/view/10.1093/acref/9780199571123.001.0001/m_en_gb0603830.
- [WGG+10] E. Wolfart, J.G.M. Gonçalves, K.H. Gutjahr, C. Listner, P. Loreaux, P. Marpu, I. Niemeyer, A. Patrono, A. Ussorio (2010): GIS based Integration and Analysis of multiple source Information for Non-Proliferation Studies. In: Proceedings of the IAEA Symposium on International Safeguards 2010, p. IAEA-CN-184/231(1-8).
- [WrYo06] D. Wrazien, M. Young (2006): Overview of ArcGIS Solutions in Service-Oriented Architectures. ESRI Developer Summit, 2006.
- [Yu11] L. Yu (2011): A Developer's Guide to the Semantic Web. Springer Berlin Heidelberg.
- [Zimm13] A. Zimmermann (2013): Functional View on the BRIDGE Architecture. Public deliverable D04.2 of the BRIDGE project.

Internet sources

- [www1] http://en.wikipedia.org/wiki/Linked_data#mediaviewer/File:LOD_Cloud_Diagram_as_of_September_2011.png
- [www2] Eurostat: Your key to European statistics. Online: <http://ec.europa.eu/eurostat/web/nuts/overview>
- [www3] ABSOLUTE Project Newsletter 2014. Available at http://www.absolute-project.eu/images/Newsletter_ABSOLUTE_2014.pdf.
- [www4] Public summary of the project. Available at <http://cope.vtt.fi/COPE%20public%20summary%20with%20figures.pdf>.
- [www5] CEN workshop agreement: Disaster and emergency management - Shared situation awareness - Part 1: Message structure. Online: https://www.oasis-open.org/committees/download.php/42411/CWA_15931-1.pdf
- [www6] Common Alerting Protocol Version 1.2. Online: <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html>