COLLABORATION IN CRISIS MANAGEMENT – LEARNING FROM THE TRANSPORTATION DOMAIN

Christian Flachberger[1], Eduard Gringinger[2], Thomas Obritzhauser[3]

[1] christian.flachberger@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria
[2] eduard.gringinger@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria
[3] thomas.obritzhauser@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria

Abstract

Cross organizational collaboration is a well-developed standard way of working within crisis management. However, the underlying information management tools today don't support integrated electronic information management in complex multi-organizational scenarios. This leads to a fragmentation of relevant information into pieces held by different stakeholders. Recently, the concept of the Common Information Space has been introduced as possible solution. This paper looks to the domain of Air Traffic Management where a similar problem was tackled by a concept called system wide information management. The paper starts with describing the operational context, the unresolved needs, and the derived requirements on possible solutions. Results and experiences from the Air Traffic Management domain are gathered and compared with current solution concepts from the public safety domain which are based on the idea of the Common Information Space. The paper concludes with learnings for the ongoing development in the public safety domain.

Keywords: crisis and disaster management, collaboration, information sharing, situation awareness, common information space, air traffic management

1 NEED FOR IMPROVEMENT OF COLLABORATION TOOLS

During the time-critical response phase within a crisis- or disaster management action, cross-organizational collaboration and the related information management today is still mostly based on face-to-face meetings, telephone calls, fax transmissions, email messages, paper charts, whiteboards, and proprietary electronic systems. We gathered this insight from our experience as supplier of control centre solutions for the public safety domain in various European member states[1]. As a consequence situation awareness and decision making is hampered by a fragmentation of relevant information into pieces held by different stakeholders. Within the highly collaborative scenarios of crisis management efforts this fragmentation causes uncertainty whether the information base for critical decisions is up-to-date, comprehensive and valid.

1.1 Operational Context

Decision making based on a comprehensive picture of the situation requires exchange, verification and integration of all the different pieces of information provided by the stakeholders with their organizational and cultural background [1]. At the same time a common understanding of the situation is also a basic pre-requisite for successful collaboration [2]. This chapter describes the stakeholders and the information involved.

---

[1] This was done within commercial projects in Norway, Germany and UK; but also within the European Research projects IDIRA [6], EPISECC [7], SEMNOTAM [16] and the SESAR programme [13]

1.1.1 Stakeholders

The stakeholders (cf. Fig. 1) are on the one hand organizations from the public safety domain where crisis management is part of their core business such as civil protection and first responders. On the other hand, also organizations play an important role whose core-business has per se nothing to do with crisis management (e.g. infrastructure operators). In case of a crisis they are required to contribute to the crisis management effort in addition to their own business continuity management [3], [2].

- → **Civil Protection**
  - – Crisis management departments on regional and national level
  - – MoI, Department of Health, Department of Infrastructures
- → **First Responders**
  - – Police
  - – Fire
  - – Ambulance
  - – Armed Forces
- → **Critical Infrastructures**
  - – Highway Agency, Railway
  - – Power Companies
  - – Telecom Providers
- → **Specialised Institutes**
  - – Geodynamics
  - – Weather
- → **The Citizens**

Fig. 1 Stakeholders of a Common Information Space (CIS) for crisis management

1.1.2 Information Involved

The information involved is generated within the four phases of the crisis management life-cycle (cf. Fig. 2). Without exchange and integration of these pieces of information the fragmentation leads to different views on the situation, different assessment of needs and priorities, and to an obstruction of the practical collaboration [4], [2] and [5].

Fig. 2 Phases of the crisis management life-cycle and information involved

1.2 Operational Requirements

Specific needs have been derived from user-group workshops especially within two European projects: IDIRA [6], EPISECC [7]. These needs where analysed from the perspective of their influence on the conceptual design of a possible solution, e.g. in form of a Common Information Space (CIS) [5] and are listed below:

1.2.1 Need for ad-hoc, closed, mission specific user-groups

End-users need to be able to define on-demand (i.e. in case of an event) mission specific user-groups for information sharing.

1.2.2 Need for Integration of information

Information from different sources may concern the same information object itself (e.g. information about the same single incident) or may concern the same class of objects (e.g. information about different incidents of the same type). There is a need to integrate these pieces of information into one homogenous data-set, which can be used for queries or aggregation. This seems to be trivial at the first glance but since there is no standardised taxonomy or ontology across organizations it is still a challenge today.

1.2.3 Need for Role- and Mission Specific views

There is a need for a user-defined, configurable filtering and prioritization of information in order to generate meaningful role- and mission specific pictures of the situation.

1.2.4 Need for Precision on Location, Time, Validity and Security

The quality of the information base is crucial for the trustworthiness, especially, when the user is not directly working with primary information, i.e. electronic information processing is applied beforehand. Additionally, information security is essential.

2 TECHNICAL REQUIREMENTS

2.1 Layers of Interoperability

As framework for structuring the requirements the "layers of interoperability" model presented by ESENET[2] (Fig. 3) is used. It describes layers of interoperability beginning with the lowest technical layer (physical interoperability) up to the highest organisational layer (interoperability of political objectives). This paper focuses on layer 2 to 4 since they are of most relevance for the design of a technical solution [8].

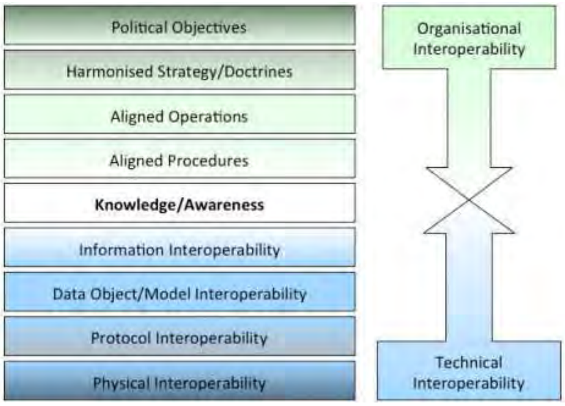

Fig. 3 Layers of interoperability according to ESENET.

2.2 Knowledge / Awareness Layer Requirements

Knowledge is seen as information which can be practically applied by a person within his or her specific context [9]. Turning information into knowledge often needs an informal sharing of views and ideas. Therefore, the basic requirement on the knowledge layer is to support this discussion process by providing a "*trading zone*" [4]. Pieces of information shared can – if required – be starting point for a discussion process.

2.3 Information Layer Requirements

Many organisations in the public safety domain are using their own, proprietary vocabulary for their communication. I.e. taxonomies and ontologies are very different and

[2] http://www.esenet.org/ Accessed 2015-06-11

it seems not likely that a common standard will be developed and adopted within a reasonable time. The basic requirement for the information interoperability layer is therefore to support a mapping between different, proprietary taxonomies [10]. At the same time existing ontologies (e.g. the tactical situation object TSO [11]) and best practises (e.g. the emergency relief items catalogue[3] of the IFRC) shall be considered.

2.4 Data Object / Model Layer Requirements

A number of well-known data exchange models is already available today. Relevant examples for domain specific models are the Emergency Data Exchange Language (EDXL)[4], including the Common Alerting Protocol (CAP)[5]; the U.S. National Information Exchange Model (NIEM)[6] or the Weather Exchange Information Model (WXXM)[7]. An example for a broadly used data model for geospatial information is the Geography Markup Language (GML)[8]. The basic requirement for the data object / model layer is to re-use these models and to provide interoperability including translation between specific models if required.

2.5 Protocol and Physical Layer Requirements

In order to fulfil the need for being able to build up ad-hoc, mission specific user-groups, the information distribution mechanisms must allow ad-hoc adding of additional partners. It must be possible to find services available within the information space (e.g. via a service registry). The specific situation of mission critical crisis and disaster relief actions requires off-line capabilities (i.e. local caching of information and automated re-synchronisation).

3 SOLUTION CONCEPTS

A number of projects within the public safety domain currently focus on solutions for a CIS. Therefore, it seems to be worthwhile looking into other domains with similar questions of collaboration. One of these domains is Air Traffic Management (ATM). Since airplanes are moving around the entire globe the necessity for developing standards and legal frameworks for information sharing has been there right from the beginning. This chapter gives an insight into solution concepts from both domains.

3.1 Solution Concepts from the Public Safety Domain

Within the public safety domain, the U.S. XChangeCore[9] programme and the ongoing European Research projects EPISECC [7], SecInCoRe[10], REDIRNET[11], SECTOR[12], IDIRA [6] and DRIVER[13] have been identified as relevant projects or initiatives, respectively. All these projects implement a Common Information Space (CIS). The CIS interconnects technical systems and applications of different organisations in order to support information sharing. The exchanged data needs to be converted since the different applications usually use owner-specific taxonomies, data formats, and protocols. In order to avoid the necessity of N-to-N conversions, the concepts are based on a set of standard protocols, data formats and taxonomies. This allows implementing N-to-1-to-N conversion models based on application specific adaptors which depend on the individual external application itself as shown in Fig. 4.

[3] http://procurement.ifrc.org/catalogue/ Accessed 2015-06-11
[4] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency Accessed 2015-06-11
[5] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html Accessed 2015-06-11
[6] www.niem.gov Accessed 2015-06-11
[7] http://www.wxxm.aero Accessed 2015-06-11
[8] http://www.opengeospatial.org/standards/gml Accessed 2015-06-11
[9] http://www.xchangecore.org/ Accessed 2015-06-11
[10] http://www.secincore.eu/ Accessed 2015-06-11
[11] http://www.redirnet.eu/ Accessed 2015-06-11
[12] http://www.fp7-sector.eu/ Accessed 2015-06-11
[13] http://driver-project.eu/ Accessed 2015-06-11

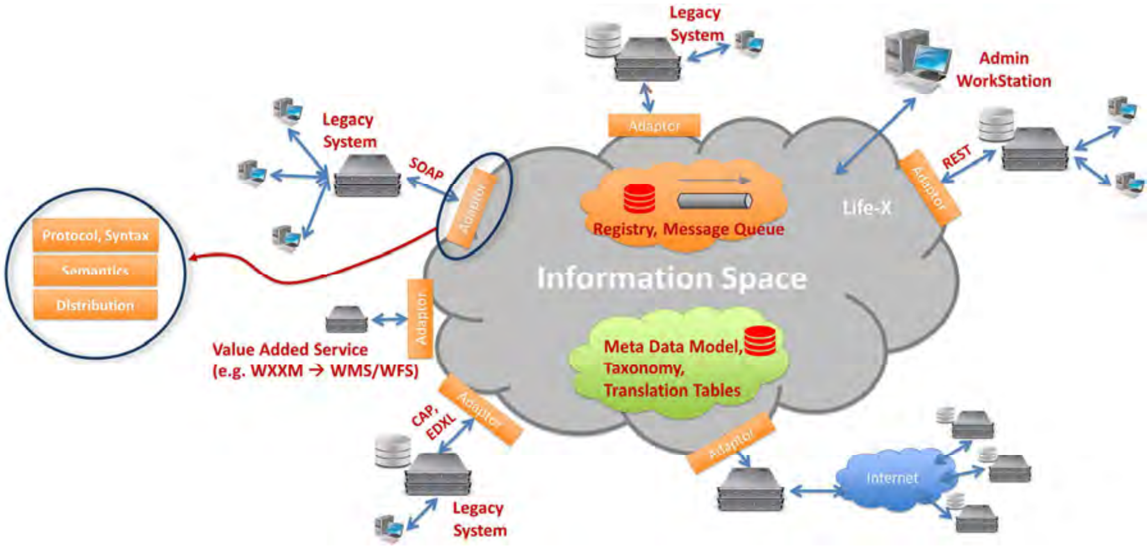

Fig. 4 Architecture of the Common Information Space (CIS)

The project C2-SENSE[14] additionally introduces profiles. Each profile defines with regard to a specific operational use which set of standards shall be used for communicating via the CIS. Referring to the knowledge/awareness layer, the project IDIRA [6] implemented a possibility to establish ad-hoc voice calls between a provider and a consumer of a certain piece of information using an application called IDIRA Webtalk. XChangeCore is based on a partially meshed network. XChangeCore servers allow clients to collaboratively assemble and share emergency management information using web services provided by their local XChangeCore server. Collaboration occurs between clients connected to one XChangeCore server transparently and between clients on different XChangeCore servers based on information sharing agreements. The Common Information Space is a data sharing platform but not a data repository. The ownership of the data stays with the applications. It doesn't provide any business logic. The validation, interpretation and processing of the transported data is part of the applications.

3.2 Solution Concepts from the Transportation Domain

Within the air traffic management domain, System Wide Information Management (SWIM) [12] including the ATM Information Reference Model (AIRM) [13], the Information Service Reference Model (ISRM) [14], and the SWIM Technical Infrastructure (SWIM-TI) [15] has been introduced. The concept of SWIM is a fundamental change of how information is managed along its full lifecycle, involving stakeholders from across the whole European ATM network. The list of stakeholders is divided into two main groups, civil and military. Under these you will find air navigation service providers, airport operators, airspace users, network managers and industry partners. SWIM is SESAR's[15] most important enabler for assuring that the right information will be available with a certain level of quality for a specific operation at the time needed [12]. It covers all ATM information, including aeronautical, flight, aerodrome, meteorological, air traffic flow, and surveillance. SWIM consists of standards, infrastructure, and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services.

The AIRM is used as a common reference and consists of an information- and logical data model capturing various domains [13]. The AIRM represents civil, military and

---

[14] http://c2-sense.eu/ Accessed 2015-06-11

[15] Single European Sky ATM Research, http://www.sesarju.eu/ Accessed 2015-06-12

hybrid information constructs relevant to ATM. The model ensures semantic interoperability within ATM and maybe will be used also on International Civil Aviation Organization (ICAO) level as ATM information standard worldwide. The ISRM describes information services needed by operational processes or operational services to fulfil their information needs [14]. The idea is to have a registry available from which the specific operational people can choose from. SWIM-TI is the technical enabler for the SWIM concept realization [15]. The main goal is to increase the common situational awareness by improving the ability to deliver the right information to the right people at the right time. SWIM-TI contributes to the services' solution aspects providing means supporting an effective and secure ATM-specific services provisioning and consumption among SWIM Enabled ATM systems. The SWIM-TI is a set of software components distributed over a network infrastructure providing functions and enabling collaboration among ATM systems. There are different profiles for different purposes available. With the commission implementing regulation No 716/2014[16] of the European Union, the legal aspects are defined for supporting the implementation of the European ATM Master Plan including SWIM in the context of the common pilot project.

4 COMPARISION AND DISCUSSION

Even though it looks as if there are nearly no overlaps between the Public Safety and Air Traffic Management Domain, the concepts presented are more alike than expected. This chapter compares and discusses the various concepts presented in section 3.1 and 3.2 in regards of similar approaches and standards used. Fig. 5 identifies the different interoperability layers of the discussed solution concepts. The semantic, syntactic, and technology interoperability layer can be found in the presented SWIM components as well (cf. section 3.2). The following sections handle those layers in detail.

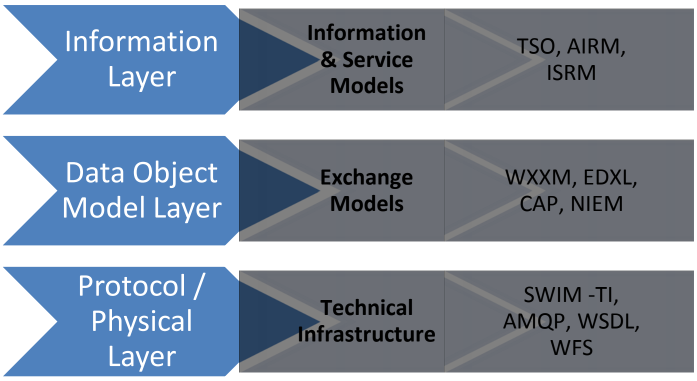

Fig. 5 Mapping the Interoperability Layers to Solution Concepts

4.1 Comparison of the Information Layer

All presented solution concepts contain a semantic layer which represents the operational knowledge of a specific domain. Within the transportation domain this layer was identified as one of the major fields of research for enhancing future interoperability and harmonization by introducing the information model AIRM and service model ISRM. In addition to the definition of business terms, also harmonized definitions for generic concepts such as geometries, temporality and identifiers are modelled. Future research programs like SESAR 2020 will further explore the semantic layer. Although a baseline has been found, future work on a common semantic reference model will be necessary within the public transport domain. In the public safety domain, this baseline has not yet been found and is currently within the scope of a number of research projects.

[16] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0716&from=EN Accessed 2015-06-11

4.2 Comparison of the Data Object / Model Layer

For each domain, a common information reference model needs to be aligned with the used exchange models and vice versa. Existing exchange models (e.g. WXXM, EDXL, CAP, and NIEM) are already used today to improve the digital communication between different stakeholders. This defines the Data Object / Model Layer. This proliferation of formats obviously increases the effort used in building a knowledge framework – inconsistent use of business terms and business rules would need to be resolved.

4.3 Comparison of the Protocol and Physical Layer

The architectural and messaging patterns described in the solution concepts are very similar (SOAP, Web Services, etc.). Each technical infrastructure uses adaptors (access points) and provides capabilities and functionalities that enable those adaptors and external service consumers/producers to participate in operation of services and information exchange. Adaptor components therefore specify service authentication and authorisation, data conversion, and other additional features. In the transportation domain different profiles support specific operational needs (e.g. near real-time transmission). In the public safety domain the solution of EPISECC and DRIVER is similar to XChangeCore except the network structure. The services are connected via adaptors to the CIS which allows the network configuration being independent from the connected application/services. C2Sense introduces a profile concept similar to the transportation domain.

5 CONCLUSION & OUTLOOK

What can we learn from the air traffic management domain for crisis management? One lessons learnt is that the challenges which the crisis management is currently facing can be mastered. Secondly, it is obvious, that the experiences cannot simply be transferred directly from the global air traffic management domain to the regionally fragmented, complex and highly dynamic crisis management domain. Taking this into account, the following learnings are proposed to be considered: A transformation from a product-centric paradigm to an information-centric paradigm is needed. The development of an information reference model (semantic layer) is necessary. Information sharing doctrines and procedures need to be introduced. Early development of applications providing a possibility to experience the user-benefits in reality will facilitate the transition. All of that should follow an iterative approach starting with a simple baseline. Existing data models should be re-used for finding the baseline where appropriate. Possible candidates are the relief items catalogue of the IFRC, the Tactical Situation Object or the Weather Information Exchange Model, but many others can be identified.

Within the European Union different strands of activity are driving the transformation forward:

Standardisation: The discourse about a concept of networked crisis and disaster management is being pushed forward by policy makers of DG Enterprise. A good example is the mandate 487[17] of the European Commission.

Focused R&D: Different research projects mentioned in this paper will contribute further by developing and demonstrating practical solutions: EPISECC, SecInCoRe, REDIRNET, SECTOR, IDIRA, and DRIVER.

Stakeholder involvement and awareness raising: Among other initiatives, the project ESENET conducts a number of workshops in different European member states and provides a structured possibility for online discussions.

[17] http://www.etsi.org/images/files/ECMandates/m487.pdf Accessed 2015-06-10

ACKNOWLEDGEMENTS

IDIRA, EPISECC, DRIVER, ESENET and SESAR are funded by the European Commission. SemNOTAM is funded by the Austrian Research Promotion Agency (FFG).

REFERENCES

[1] W. Treurniet and et al., "Governance of occasional multi-sector networks," in *Proceedings of the 11th International ISCRAM Conference*, University Park, Pennsylvania, USA, 2014, pp. 118 - 122.

[2] J. Morentz, "Unified Incident Command and Decision Support (UICDS): A Department of Homeland Security Initiative in Information Sharing," in *Conference on Technologies for Homeland Security*, Waltham, IEEE, 2008, pp. 321 - 326.

[3] V. Atluri and et al., "UICDS-based information sharing among emergency response application systems," in *Proceedings of the 12th Annual International Digital Government Research Conference*, New York, ACM, 2011, pp. 331-332.

[4] K. Boersma and et al., "Negotiating the 'Trading Zone'. Creating a Shared Information Infrastructure in the Dutch Public Safety Sector," *Journal of Homeland Security and Emergency Management,* vol. 9, no. 2, 2012.

[5] N. Selvaraj and B. Fields, "Developing a Framework of Common Information Space (CIS): Grounded Theory Analysis of Airport CIS," in *Collaboration and Technology*, Berlin Heidelberg, Springer, 2010, pp. 281-296.

[6] Fraunhofer, "IDIRA Interoperability of data and procedures in large-scale multinational disaster response actions - Final Report," 13 05 2015. [Online]. Available: http://www.idira.eu/. [Accessed 08 06 2015].

[7] e. a. Huebner, "Towards a Pan-European Information Space," in *Proceedings of the ISCRAM 2015 Conference - Kristiansand, May 24-27*, Kristiansand, Palen, Büscher, Comes & Hughes, eds., 2015.

[8] H. Kubicek and et al., "Layers of Interoperability," in *Organizational Interoperability in E-Government*, Berlin Heidelberg, Springer, 2011, pp. 85-96.

[9] J. Hey, "The data, information, knowledge, wisdom chain: the metaphorical link," *Intergovernmental Oceanographic Commission,* 2004.

[10] H. C. Siddharth Kaza, "Evaluating ontology mapping techniques: An experiment in public safety information sharing," *Decision Support Systems,* vol. 45, no. 4, 2008.

[11] D. R. Fedra Henriques, "OASIS Tactical Situation Object: a route to interoperability," in *SIGDOC '08 Proceedings of the 26th annual ACM international conference on Design of communication*, New York, ACM, 2008, pp. 269-270.

[12] P. Single European Sky ATM Research (SESAR) Programme, "SWIM conops, edition 00.04.05," SESAR Joint Undertaking, Brussels, 2014.

[13] P. Single European Sky ATM Research (SESAR) Programme, "AIRM Primer, edition 03.03.01," Sesar Joint Undertaking, Brussels, 2015.

[14] P. Single European Sky ATM Research (SESAR) Programme, "ISRM Primer, edition 00.05.00," SESAR Joint Undertaking, Brussels, 2014.

[15] P. Single European Sky ATM Research (SESAR) Programme, "SWIM TI definition, edition 00.02.00," SESAR Joint Undertaking, Brussels, 2014.

[16] F. Burgstaller, E. Gringinger, D. Steiner, M. Schrefl, S. Wilson and S. v. d. Stricht, "AIRM-based, Fine-grained Semantic Filtering of Notices to Airmen," in *Integrated Communications, Navigation and Surveillance Conference*, Washington, 2015.