Interoperability and Formal Concept of Radar Systems as Clouds

Mehmet Emre ÇİFTÇİBAŞI

eciftcibasi@stm.com.tr,

Yusuf Egemen BAŞKARAAĞAÇ

ebaskaraagac@stm.com.tr,

Özgür GÜLERYÜZ

oguleryuz@stm.com.tr

STM Inc.,
Ankara Teknoloji Geliştirme Bölgesi,
Bilkent 5. Cad. No: 6/A,
Bilkent, Ankara,
TURKEY

ABSTRACT

Interoperability of maritime systems requires the language of the shared information to be compromised by all parties. Radar systems are mainly known as situational awareness systems, which enable the perception, comprehension and projection capabilities of the real world from semantic view of information systems. Maritime domain awareness requires many capabilities which can only be achieved by all source integration of maritime related systems, generation of national maritime data model and automation of systems by enabling formal concept analysis (FCA). Formal concept analysis is proposed as the core of decision support and anomaly detection in maritime domain. Concept lattices are generated and concept exploration methods are utilized on maritime ontology for maritime domain awareness requirements of the nation. The proposed framework aims to achieve maritime domain interoperability in a sense of an electronic library approach.

Within the maritime electronic library, the core architecture is considered as a cloud computing architecture. The cloud architecture enables us to reach many services via Software as a service (SaaS). The SaaS cloud architecture enables the interoperability of different government agencies' radar and information systems by web based maritime information system interfaces. For satisfying the interoperability requirements of the different government agencies, the agencies need to have their own analysis tools for analyzing the maritime context. These tools will have different capabilities for analyzing and reporting the maritime events. No such tool can satisfy the requirements of all government agencies, so these tools need to be designed separately but all will have access to the same maritime context via the cloud architecture, enabling different analysis capabilities. The SaaS cloud architecture is also modeled via the use of a Service Oriented Architecture (SOA), mainly for maritime domain interoperability data distribution and governance capabilities of Enterprise Service Bus (ESB).

1.0 INTRODUCTION

Maritime domain consists of multi disciplinary sub domains, where these sub domains are represented by different civilian and military agencies. These agencies need to use the maritime data in their own perspective, having similar maritime information sharing requirements. The maritime related information shall be generated and shared in a maritime interoperability cloud. The interconnection of maritime data is best realized by Software as a Service (SaaS) architecture, avoiding the duplication of data, workforce and infrastructure costs. A very important aspect of generating and distributing maritime information is the extraction of mission critical data from many connected databases in near real time, which in turn requires the systems to be fully interoperable for further analysis.

In this paper, we introduce the concept of maritime domain interoperability and define the common maritime ontology and data model for making these sub domains interoperable. We hereby define the maritime data model as the main requirement for enabling the integration of any two or more information systems while protecting the semantics of each system. We focus on the automation of maritime systems and introduce the concept of anomaly detection in maritime domain. Then we propose a theoretical approach for Maritime Situational Awareness (MSA) concept analysis by defining maritime ontologies as context, utilizing concept exploration as a tool for dynamically aligning the MSA concept lattice.

Afterwards we define the maritime interoperability cloud architecture within the advantages of community cloud. The consumer approach of different maritime agencies, probable services supplied by the architecture and its advantages. Lastly, we finalize the paper by service oriented architecture decision criteria and conclude with our suggestions and requirements for establishing a maritime information system.

2.0 INTEROPERABILITY REQUIREMENT FOR MARITIME INTEGRATION

Interoperability of maritime related agencies requires the semantic communication between member nations' maritime information systems. NATO definition of interoperability is “The ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives” and the NATO Architecture Framework (NAF) defines interoperability as “The ability to operate in synergy in the execution of assigned tasks” [1]. Consequently, to enable the national information systems to act together and operate in synergy, information systems need to share information semantically for increase in automation and detection of anomalies. The semantics of information shall be protected while information sharing takes place.

The maritime related data is stored in different systems in national agencies and currently many agencies are accessing the data from their own interfaces. To enable the nationwide maritime domain interoperability, maritime system interfaces shall be integrated through a semantic interoperability layer, which requires the generation of a common maritime data model. The maritime data model shall provide the semantics of information sharing by a common maritime ontology, which will be capable of protecting the “meaning” of shared data between systems.

3.0 THE GOAL: ANOMALY DETECTION

Maritime domain consists of several multi-disciplinary branches, each of which deals with completely different and huge amount of data sets. To achieve MSA, each data set needs to be thoroughly analyzed and cross linked by a formal way. The results of the formal analysis are to be used in not only improving the daily operations such as optimization of maritime commercial vessel routes against illegal trafficking, but also for maritime anomaly detection.

Anomaly detection refers to detecting patterns in a given data set that do not conform to an established normal behavior. The patterns thus detected are called anomalies and often translate to critical and actionable information in several application domains. In maritime domain, a vessel coming from Country A, with a load of Substance 1, may be referred to as a normal behavior, while the same vessel coming from Country B with a load of Substance 1 may be referred to as an anomaly. Our main effort in this paper is to automate the detection of anomalies in maritime domain, through the analysis of the knowledge base generated by domain experts. The knowledge base shall be temporally updated according to new maritime incidents, such as the same vessel coming from Country A with a load of Substance 1 may be referred to as an anomaly by time, if the ship gains a criminal record.

Supposedly, a cargo vessel V1, coming from country U1 with a load of S1 is a normal behavior. But later on, the law enforcement receives a notice stating that the load is not S1, but illicit cargo. After this event, all cargo vessels coming from country U1 with a load of S1 becomes an anomaly for a predefined time frame, keeping in mind that the suspicion includes all known related commercial routes, vessel personal lists and ship owners.

This suspicious behavior of all related vessels need to be analyzed and all vessels of interest shall be classified into a set of suspicious vessels, each set containing a different property of vessels such as vessels from Country U1, ships with crew C1, ships with load of S1. We need to find a formal way for creation of data sets and a graphical way of navigation through these sets so that we can focus on the suspicious vessels and semi-automate the anomaly detection process. For the arrestment of the offenders in maritime domain, the maritime governmental authorities need to gather all maritime related data into a database, and the information in the database shall be automatically analyzed 24/7 for suspicious behavior, helping the law enforcement operations. One procedure for behavioral analysis by the usage of the time varying knowledge base is called Formal Concept Analysis.

4.0 THE TOOL: FORMAL CONCEPT ANALYSIS

Formal concept analysis is a theory of data analysis which identifies conceptual structures among data sets, by usage of contexts and concept lattices [3]. This method intends to make ontology building more efficient and allows for discovering necessity for new concepts and relations in an ontology, which leads to an ontology that has these entities described in a way suitable for knowledge exchange. Member nations' semantic information sharing objectives and interoperability goals will be achieved by forming the maritime ontology from the formal context and analysis of the concept lattice near real time [4]. The cloud architecture, detailed in section 5, will be used for interconnection of the radar clouds and databases.

4.1 FORMAL CONTEXT

Before analyzing and sharing the maritime information, all the vessels and properties shall be listed in a worksheet composed of two dimensional tables, for machine readability. The tables shall have related objects in rows, and attributes in columns. For easy machine processing, we shall form the context such that, the context includes the objects' attributes by a simple relation, instead of a complex ontological definition [5].

We will create a maritime ontology, which is simple to process, but detailed enough to include all related maritime information in the formal context of the maritime domain. We will form the worksheet consisting all these tables, and we will be able to browse through the worksheet from a graphical user interface, which will give warnings in pre-defined events and anomalies, such as "Person P3 (Criminal), on a vessel that carries cargo (S1), from Country U1", based on the previous experience of domain experts. This anomaly detection will be the decision support algorithm of the SaaS architecture. The anomalies will be reported to the user via Service Oriented Architecture so that the law enforcement agencies can take appropriate action. The ontology is similar to examples from [6], [7].

4.2 CONCEPT LATTICE AND EXPLORATION

Concept lattices are used to represent conceptual hierarchies which are inherent in data. They are the core of the mathematical theory of Formal Concept Analysis (FCA). There are many algorithms to build concept lattice, while in our work of maritime ontology building, we will focus on the requirement for a graphical user interface for concept exploration.

Suppose our aim is to find the suspected vessel in a set of all vessels. With domain experts help, the system "has learned" the suspected vessel criterions. We construct the concept lattice with previous experience of the domain experts, as in Figure 1.

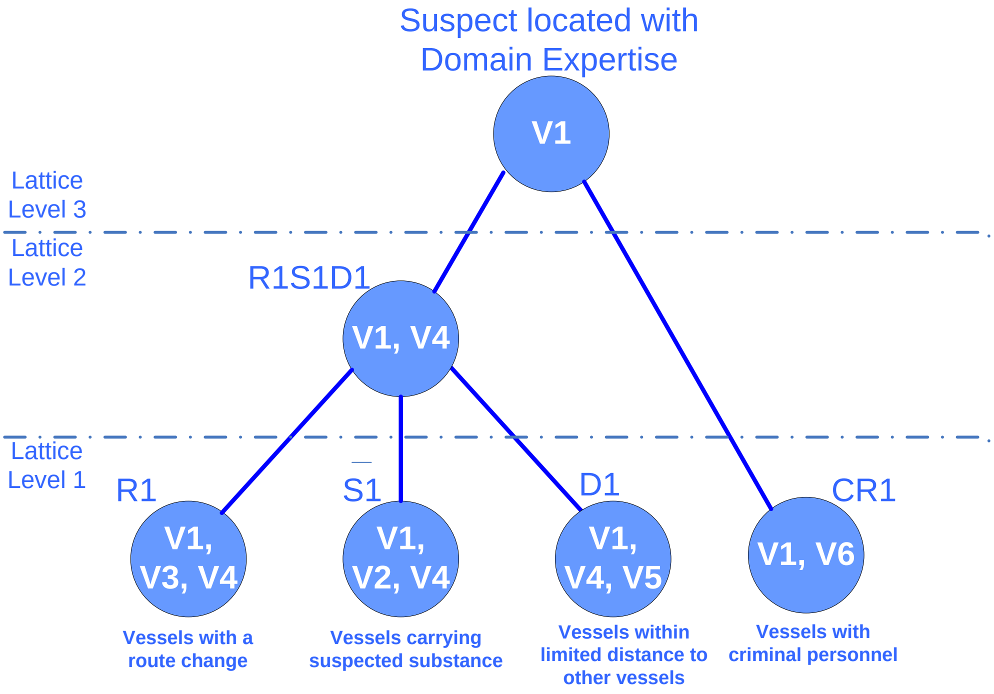

Figure 1: Suspect Location with Domain Expertise via Concept Lattice

This connection of sets enables multi level generation of concept lattice, which in turn returns a limited set of vessels, where this limited set enables the operator to physically examine the vessels in the set for illegal activities. Additional levels can be generated by forming new concepts and connecting them, which in turn results very limited number of vessels, even more possible for physical inspection.

The operator can watch some concepts for newly added vessels, and the system can generate alerts for each vessel addition to these concepts. These concepts may act as the main decision support module of the maritime information system, and the knowledge of domain experts play a very important role. By time new sets can be generated, as new expertise is gained by law enforcement activities and the system learns to catch maritime anomalies in time.

Now that we have formed our concept lattice, we need to use the graphical user interface for concept exploration, also known as relational browsing [8]. This latter stage of formal concept analysis, aims to find new concepts, new sets of vessels, that might be advantageous to investigate for law enforcement agencies. After drawing the simple concept lattice, suppose we have new sets of ships:

Vessels carrying explosive (S1): V1, V2, V3, V4, V5, V6,

Vessels coming from country one (U1): V1, V3, V5, V7, V9, V11

Vessels with criminal personnel (CR1): V1, V2, V6, V10

We explore a new concept, by intersecting the S1 and U1 sets, and find the concept S1U1 with elements V1, V3 and V5, then intersect this set with criminal personnel set CR1 to find the concept with only element V1.

If the result V1 does not satisfy the operator, or is known to be a regular vessel, then the law enforcement needs to find new sets of vessels for inspection. Concept exploration becomes critical here, where we will explore the concept lattice for new concepts.

The need to find new suspected vessels drives the need to find new sets/concepts. The most common method of finding the new concepts is asking the Question to the set S1U1: "What common properties do the subsets of this concept/set have?" Suppose we get the answer "%90 of the members of the concept S1U1 carry TV". Then the system can suggest inspecting a new concept from the initial set of vessels, namely a set of vessels carrying TV, which is a regular load for commercial vessels, but can be used in illegal activities. Then we can find the intersection of this set with the set of personnel with criminal records (CR1) by operators' domain experience. The intersection of this concept with concept CR1 gives the set of suspicious vessels V1 and V10 as a result. Reaching V10 is important here, as the system suggested the operator a new vessel for inspection. More common properties of this concept can also be inspected for further analysis, along with the other common properties of the concept S1U1. The concept exploration is shown in Figure 2: Concept Exploration for automatic suggestion of a new suspected vessel.

The same operation can be done for other common properties of the concept S1U1, such as "%75 of the members of the concept S1U1 are en route to country U2". Then similarly, a new concept can be initiated from the initial set of vessels, namely a set en route to country U2, and further analysis can also be performed on this and similarly generated sets.

The system will aid the operator by tightening the sets of suspected vessels, and gives the law enforcement agencies a chance to catch the anomalies. The graphical user interface helps the user to use the computing power of servers for browsing through the vessels and minimizing the set of suspected vessels. Formal generation of the context enables the system for near real time formal concept analysis.

A very important requirement of the system described here is to keep the context tables updated from the databases. The system needs to get the required data from the connected databases and generates the tables online. To enable the system for performing formal concept analysis, the updated tables need to be generated and stored with timestamps in a data storage unit, centrally or distributed.

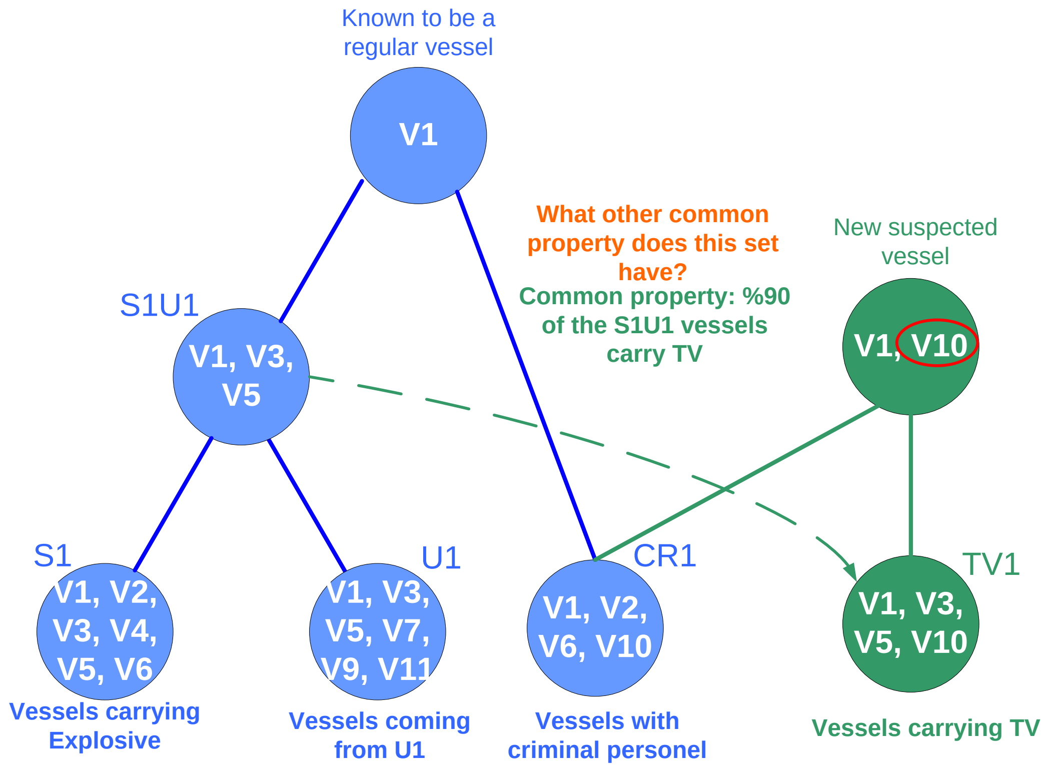
Known to be a regular vessel
V1
What other common property does this set have?
Common property: %90 of the S1U1 vessels carry TV
New suspected vessel
S1U1
V1, V3, V5
V1, V10
S1
V1, V2, V3, V4, V5, V6
U1
V1, V3, V5, V7, V9, V11
CR1
V1, V2, V6, V10
TV1
V1, V3, V5, V10
Vessels carrying Explosive
Vessels coming from U1
Vessels with criminal personel
Vessels carrying TV

Figure 2: Concept Exploration for automatic suggestion of a new suspected vessel

5.0 THE INFRASTRUCTURE: CLOUD COMPUTING

Maritime management goals of nation, has led to the government agencies with distinct responsibilities, and these responsibility areas are classified into four main sub domains as, 1. Maritime Security, 2. Maritime Navigational Safety, 3. Maritime Environmental Protection and 4. Maritime Economic Affairs. Actually these four sub domains are interpenetrated into each other from operational perspective, and need to be connected within the system architecture definition. We hope to connect the four sub domains and their situational awareness sensors and databases by cloud computing architecture, as shown in figure 3.

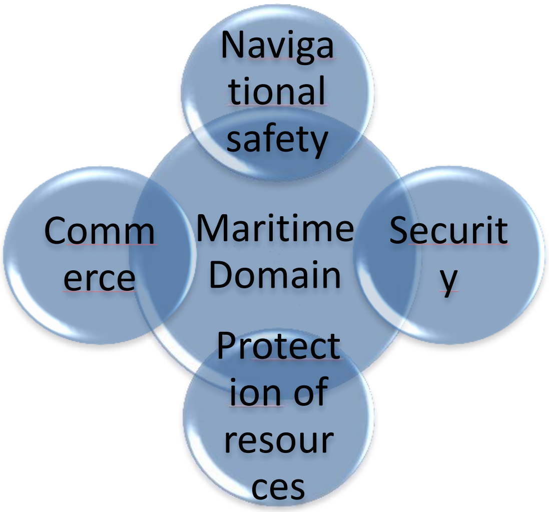

Figure 3: Maritime Interoperability Cloud

Cloud computing not only enables the virtualization of hardware and software but also lowers the management and service provider costs. Cloud architecture uses configurable resources from the shared pool of IT infrastructure, utilizing resources only when users require access.

Cloud infrastructure is developed as a three layered architecture: infrastructure, platform and services. The infrastructure consists of physical and virtual resources such as sensors, databases, computational capabilities, virtual network servers and so on. The platform is composed of API, web interfaces, scripts and libraries. The services layer is formed by the applications serving alliance, corporate, academic or social requirements.

The advantages of cloud computing in maritime interoperability is similar to the civilian applications. The most important aspect of the maritime cloud is wide network support and independent resource pool through entire country. The maritime domain will have a user from the related government agencies in each military or civilian port.

The elasticity of cloud computing will enable the maritime information system to serve new government agencies in time. The maritime information system community cloud will enable the data sharing between government agencies, enabling a better operational process for interoperability. Critical information will be transferred between agencies and data analysis defined in previous section will be performed on this information. The national technological investments will be optimally used, thus reducing the operation costs.

5.1 SOFTWARE AS A SERVICE FOR INTEROPERABILITY OF RADAR SYSTEMS

In 21st century, all government agencies have accepted that the future of MSA is interoperability. All agencies have different sensors for MSA. Some agencies have radar systems for surveillance, some has radios for communication with vessels and some has databases for identification, criminal and economic information of vessels. The most important aspect of MSA forming the maritime cloud is the usage of previous national technology investments for interoperability. All these information sources need to be connected in such a way that we can detect the suspected vessel and perform the analysis described in the previous sections of this paper. We hereby use the name maritime information system, for the cloud architecture enabling the interoperability of radar systems and databases.

There are many challenges on the way to the all source integration of the maritime information system. Most of the agencies tend to act slowly, as they have not used the maritime information system previously. The main reason is the cost of replacing their legacy IT architectures and complexity of integration to new IT systems. The Software as a Service (SaaS) concept steps forward as a promising solution for interoperability of radar systems, by its low installation costs and ease of integration.

SaaS architecture requires no previous IT infrastructure, except one server installed in the agency’s IT domain for connection to the community cloud, leading to low total cost of ownership. The excellent service quality and availability via the cloud architecture and the independence from geographical location by web based geographical information system; make the SaaS architecture the perfect choice for any maritime information system.

The government agencies will be consumers of maritime information system and by time their usage and effectiveness of the system will increase. The analysis capability defined in the previous section will enable the port authorities to work together with law enforcement agencies. The elasticity of the cloud infrastructure will enable nationwide optimum usage of maritime network resources and IT personnel. Virtualized servers will be cheaper and faster as they will serve all of the community cloud. As a result, the maritime information system will have many services for the “consumers”.

5.2 SAAS ADVANTAGES

As new agencies are added to the cloud, the SaaS architecture will enable many new services to its consumers. These services are used by the consumer agencies and form the main data flow of maritime information. Not only the radar plots and tracks will be distributed by cloud services, but also the vessel related data and interrogations will flow in the cloud infrastructure.

The database infrastructure of the system will allow authorized users to store information on the cloud by metadata objects while these objects can be accessed anytime anywhere by the usage of web services. Elastic compute cloud will perform anomaly detection while analysis resource optimization will be performed in the SaaS architecture. The users will send messages from the cloud and by these messages; vessel identification can be performed as a service in the cloud, enabling the most important IT achievement for the law enforcement agencies. Geographical distances between agencies will tend to decrease by the increasing usage of SaaS, and all operations in the maritime domain will be interoperable.

5.3 SERVICE ORIENTED ARCHITECTURE

The maritime interoperability requirements of the nation will be satisfied by integration of all related government agencies’ operational processes among with their IT systems. The future of integration is both the ease of data sharing and operational process sharing. The maritime information system will consist of a few agencies in the beginning but the count will increase by time. Also each agency will connect more databases and applications to the cloud in the medium term.

The Service Oriented Architecture (SOA) will allow new developed applications to seamlessly integrate to the cloud. Many commercial solutions exist in the market for the SOA infrastructure. For our maritime information system, we will install an enterprise service bus, and connect the related agencies' IT systems by web services.

As the system will prove its high level of operational performance, the maritime information system “consumers” will increase by time. Many new agencies will join the system, which will only require the definition of new web services and re-configuration of the existing ones, by publish-subscribe methodology.

The main SOA product decision criteria are the cost and performance. These criteria lead us to use a SOA product that has low total cost of ownership while supplying enough data flow with some governance and support capabilities.

6.0 CONCLUSIONS

This paper has described a novel mechanism for maritime domain interoperability and formal concept. Integrating maritime radar systems with FCA of databases via cloud computing architecture creates a new era for interoperability.

For the systems to be interoperable, they must share information without the loss of semantics, which in our case without the loss of relations to other objects and attributes. The maritime context is the viewpoint of each agency for maritime environment. After the systems reach the required information, they will process the information individually for each system's own requirements.

For the goals of the maritime domain interoperability to be achieved, the government agencies need to have their own analysis tools for processing the maritime context. These tools will have different capabilities for analyzing and reporting the maritime events. No such tool can satisfy the requirements of all government agencies so the maritime context shall be shared as an electronic library, and each agency will process the information in the library as necessary.

Maritime environment is very complicated as mentioned in previous sections and requires the integration of many systems. Some of these systems are surveillance systems, while some are online local/international databases for maritime related information. Successful all source integration of these different systems require very customized solutions including the development of a common data model [9], a mechanism similar to Semantic Interoperability Logical Framework (SILF) [2], [10], [11], [12], [13] for connecting national maritime systems.

The cloud architecture will enable anomaly detection, which is the ultimate goal of maritime related law enforcement agencies. The agencies will use the SaaS infrastructure, and all national/alliance sensors may be integrated to the cloud architecture, as necessary. The geographical distances will no longer affect the operational processes as the IT infrastructure will allow maritime information to flow all the way until it reaches its final destination, “the consumers”.

Many different operational services will be available on the maritime community cloud, and web services will be used for integration. As a result of the usage of cloud infrastructure and FCA as a tool, the maritime interoperability objectives shall be reached.

In the latter stages of our work, we will detail the interoperability advancements in maritime domain. The future work of our concept will be interoperability of national systems with EU CISE and NATO C2IS.

7.0 REFERENCES

[1] NATO TIDEPEDIA, https://transnet.act.nato.int/WISE/maritimeDo/RelatedLin/TidepediaA

[2] "Position Paper on Framework for Semantic Interoperability", NATO IST Panel Research Task Group IST-094 / RTG-044 Position Paper, July 2011.

[3] Formal Concept Analysis, http://en.wikipedia.org/wiki/Formal_concept_analysis

[4] "Formal Concept Analysis in Information Science." In: Cronin, Blaise (ed.), Annual Review of Information Science and Technology. Vol 40, 2006, p. 521-543.

[5] "Using Formal Concept Analysis For Maritime Ontology Building", 2010 International Forum on Information Technology and Applications, Liu Ning, Li Guanyu, Sun Li, 03.08.2010, Dept. of Information Science and Technology, Dalian Maritime University.

[6] "Categorization of Maritime Anomalies for Notification and Alerting Purpose", NATO MSA 2009 Paper, Jean Roy, Michael Davenport, 27.07.2009, Defence R&D Canada – Valcartier, Salience A. Inc.

[7] "Automated Reasoning for Maritime Anomaly Detection", NATO MSA 2009 Paper, Jean Roy, 27.07.2009, Defence R&D Canada – Valcartier.

[8] "Conceptual Knowledge Processing with Formal Concept Analysis and Ontologies", ICFCA, volume 2961 of Lecture Notes in Computer Science, page 189-207. Springer, (2004), Philipp Cimiano, Andreas Hotho, Gerd Stumme, Julien Tane, Institute for Applied Informatics and Formal Description Methods (AIFB), University of Karlsruhe.

[9] "The Technological Developments in Turkey Regarding Maritime Security", International Workshop on Maritime Security and Defense Against Terrorism, NATO COE DAT, Yusuf Egemen Başkaraağaç, Serhat İnan, Mehmet Emre Çiftçibaşı, 08.11.2010, STM Inc, Turkey.

[10] "A Framework For Maritime Domain Interoperability with Formal Concept Analysis", (IST-101/RSY-024) Semantic And Domain-Based Interoperability Symposium, NATO RTO, Mehmet Emre Çiftçibaşı, Yusuf Egemen Başkaraağaç, Süleyman İnci, Yüksel Erdoğan, 07.11.2011, STM Inc, Turkey

[11] "Interoperability For Maritime Security With Formal Concept Analysis", (SCI-247), Systems Concepts And Integration (SCI) Panel, Port and Regional Maritime Security Symposium, NATO RTO, Yusuf Egemen Başkaraağaç, Mehmet Emre Çiftçibaşı, 21.05.2012, STM Inc, Turkey

[12] "Automation Of Maritime Information Systems – Users Becoming Analysts", (SET-183 / IST-112), Sensors & Electronics Technology (SET) Panel and Information Systems Technology (IST) Panel, Joint Symposium on "Persistent Surveillance: Networks, Sensors, Architecture", NATO RTO, Yusuf Egemen Başkaraağaç, Mehmet Emre Çiftçibaşı, 30.04.2012, STM Inc, Turkey

[13] "Deniz Bilgi Sistemlerinde Birlikte Çalişabilirlik, Otomasyon Ve Analiz", 6. Savunma Teknolojileri Kongresi (SAVTEK 2012), SSM/ODTÜ, Mehmet Emre Çiftçibaşı, Yusuf Egemen Başkaraağaç, 22.06.2012, STM A.Ş, Türkiye