Taxonomy for Port Security Systems

Tove Gustavi and Pontus Svenson
Swedish Defence Research Agency
SE-16490 Stockholm, Sweden
Email: {firstname}.{lastname}@foi.se

***Abstract*—In this paper we describe the construction of a taxonomy for port security systems that we performed as part of the EU FP-7 project SUPPORT (Security UPgrade for PORTs). The purpose of the taxonomy is to enable port stakeholders to exchange information and to provide them with computer-based automatic decision support systems, assisting the human operator in the assessment of threat levels for a number of pre-defined threats. The decision support system uses text based automatic reasoning and high-level information fusion to identify threat indicators in the input data. Thus, the existence of a taxonomy containing well-defined terms that can be used by the reasoning system is essential. In the paper we describe the method used to construct the taxonomy, viz. first constructing a draft taxonomy and then gathering feedback on this using questionnaires. The questionnaires were motivated by the necessity to embody experience and knowledge from different groups of people involved in the project, most of which are not used to formally defining their vocabulary. Over-all, the method proved to work well and produced the expected result, namely a basic taxonomy that can be used by a decision support system, and that can be extended during the project according to need.**

I. Introduction

Europe is dependent on its ports for providing the resources needed to support our modern lifestyle. In addition to import of consumer goods and various foods, our industry depends on both the import of raw materials and the export of finished products once they have been produced. A large port such as Rotterdam handles more than 400 metric tones of cargo each year. In addition, Europe is critically dependent on ports and sea transport for its energy supply – oil and liquified natural gas are imported in vast quantities. About 40% of all freight moves in Europe take place on ships – most of them on inland rivers and canals.

There are several ways that the supply of goods to, from and within Europe could be threatened. In addition to natural disasters which can cause delays or completely disrupt a supply chain corridor, there are many ways in which antagonistic opponents can disrupt the supply chain. The most important problem for port operators and other supply chain actors is theft. Organized crime is today trying to get access to ports and containers contained within the ports and there is a strong need for preventive actions. Terrorists also pose threats to ports, both directly to them as a way of disturbing the supply of goods to Europe and indirectly by using the supply chain as a way of smuggling dangerous substances (explosives, chemicals, radioactive material) into Europe.

In the SUPPORT [1] project (Security Upgrade for PORTs), funded by the European Commission under Grant Agreement number 242112, FOI and several European partners are developing ICT-based support tools that will help increase the security of ports. The SUPPORT project focuses on antagonistic threats and will perform four demonstrations in different European ports. The work presented here focuses on the demonstration that is planned for the Port of Gothenburg, though the development of the port security taxonomy was aimed at constructing a general taxonomy applicable in all ports.

As a guide for the development of ICT tools, a SUPPORT Manual listing the eleven most important enhancement areas of Port Security was developed. The eleven ares are:

1) Managing security
2) Threat and vulnerabilities assessments and control measures
3) Access control
4) Inspections at access control
5) Screening of staff
6) Standards for fencing, alarm systems and CCTV
7) Monitoring and surveillance performances
8) Handling of cargo in cooperation with Customs
9) Checking of personnel at the facility
10) Training and awareness programs
11) High resilience concepts

There are several reasons for why it is necessary to construct a port security taxonomy. In this paper, we focus on the use of it in the decision support system, but it will also be used in tools developed for information exchange and support for threat and vulnerability assessment.

In the SUPPORT project, much of the work is based on the concept of loss events. A loss event is an event that causes loss to the port, for example theft or a terrorist attack. Figure 1 shows a schematic view of how information about a loss event (for instance in a port), its initiating events and consequences is collected by sensors and further processed in order to produce tags and indicators for use in a threat reasoning system. Of course, the idea of using automatic or semi-automatic reasoning in a decision support system is that it should make it easier for a human operator to detect a threat before anything serious has actually occurred, so that he or she can take appropriate action to prevent the threat from being realized. In addition to monitoring different threats, the decision support system should assist the operator in both preventing threats and, when this is not possible, minimizing the consequences of a loss event. This is referred to as risk control management (RCM) and will be further discussed in Section II.

To be able to reason about and classify threats automatically, a standardized set of terms a taxonomy must be used. This paper describes the taxonomy used in the SUPPORT

978-0-7695-5008-4/13 $26.00 © 2013 IEEE
DOI 10.1109/ARES.2013.78

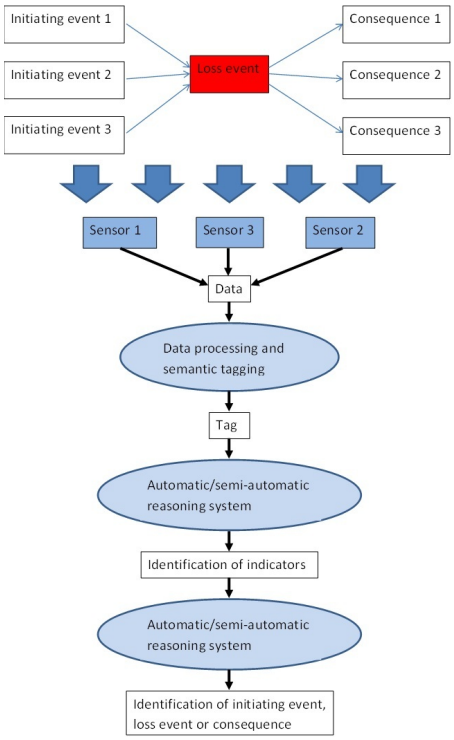

Fig. 1. A schematic overview of the text based reasoning system used in the SUPPORT project. The chain of events preceding and following a loss event gives rise to a series of sensor recordings. Sensor data is semantically tagged and used to reason about indicators and threat levels.

project. In general, a taxonomy used in a threat reasoning context must cover both identified threats, different attributes associated with the threats and tags/labels that can be used for classification of information. Other categories of terms that can be relevant to include are types of information sources and means of Risk Control Management. In the SUPPORT project, the taxonomy forms the basis of a set of shared ontologies (mappings) that define the relations between the ontologies used by the intelligent data processing and the information fusion/decision support system. A detailed discussion about the use of ontologies for increased situation awareness can be found in [2].

II. Risk Control Management

An important part of the day-to-day work in commercial ports is about preventing threats and, when this is not possible, minimizing the consequences of potential loss event (see Figure 2). The technical term for this work is *risk control management* [3]. In this paper, a *threat* is considered to be a circumstance or an event that may cause a specific security incident or a more severe (loss) event. If there is no potential loss, there is by definition no threat. Depending on the nature of the threat, the incident/event may be classified as an accident, an attack or a criminal act. Accidents fall outside the scope of the SUPPORT project.

An *initiating event* is an event that may lead to the realization of a threat. The available means that can be used to affect a threat once an initiating event has occurred are called *risk control measures*. Control measures are either *preventive*, *i.e.*, lowering the probability of the initial event to occur and initializing the loss event, or *mitigating*, *i.e.*, lowering the impacts of a loss event that has occurred. Risk control measures are often included in emergency plans, etc., and need to be verified by domain experts. Early detection of initiating events and efficient handling of the risk control measures are central for the Port Security System, which is described in Section IV. In particular, the Port Security System will focus on detection of initiating events.

In practice, initiating events are often not directly observable but have to be inferred from observations of various *indicators*. For instance, an indicator could be a certain event taking place in the port facility. To be able to reason about threat levels, the decision support system must have access to a structured set of relevant terms describing not only the port facility and the port specific routines, but also the indicators that can be used to detect the threats. In the planning phase of the risk control management work, so called *Bow-Tie diagrams* are sometimes used to structure and display the relations between initiating events, indicators, loss events and consequences. Because of the intuitive representation of information, Bow-Tie diagrams are suitable for use as starting points for identification of the threat attributes and the available means for risk control management, as described in Section V. An example of how Bow-Tie diagrams can be used for risk management in a port domain is given in [4]. An example of a Bow-Tie diagram is shown in Figure 3.

III. Background on Decision Support Systems

The Port Security System described in Section IV is essentially a decision support system. A decision support system is a computer-based system that helps decision makers structure and compile data so that patterns, relations and other features that may be important for a certain decision emerge more clearly from the available data set [5], [6]. Some decision support systems merely assist the operator in filtering out relevant information while other systems may go as far as to suggest a best solution for a specific problem. However, a decision support system, by definition, does not provide automated decision making. On the contrary, in this context decision making is seen as a process in which interaction between the operator and the system is central. A key feature of a decision support system is that the expertise and experience of the human operator is incorporated in the modeling and the analysis. Thus, it is essential that the terms used by the decision support system are familiar to the operator. This provides a strong motivation for incorporating experience from port personnel and other domain experts in the construction of the taxonomy.

The concept of *situation awareness* [7] is closely related to the process of decision making. An understanding of the current situation is needed to identify possible courses of action, and the ability to make projections into the future is crucial when it comes to predicting the effects of different decisions. Most research on situation awareness focuses on domains in which people have to make critical decisions in complex and dynamic environments. Examples of such domains are emergency response operations, military operations and air traffic control. Another type of domain in which

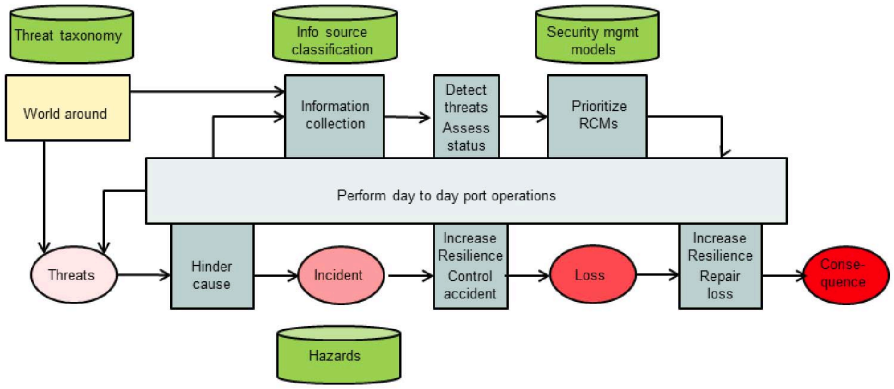

Fig. 2. The figure shows the development of an accident (red ovals) together with the risk control management functions (light green background colour) that are put in at different stages of the development. The database symbols show various static data repositories.

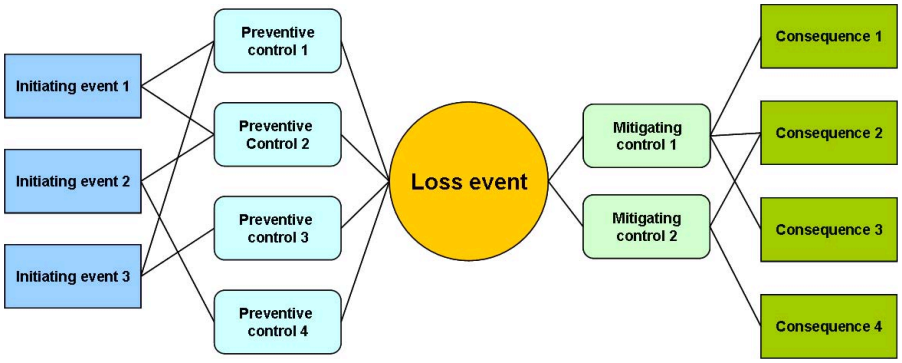

Fig. 3. Bow-Tie diagram for threat analysis.

situation awareness is important is surveillance. Surveillance differs from the above mentioned domains in that the normal situation is usually less time-critical and stressful, but even a small misjudgment of the situation at the wrong occasion may lead to severe consequences. In the above mentioned domains, decision support tools are already used in varying degrees to enhance situation awareness of both staff and responsible decision makers. In emergency response and military operations, decision support tools can for example be used to automatically extract geographical information from text documents and visualize it on a map using easily understandable graphical symbols. In surveillance, decision support tools can assist human operators in the monotonous task of monitoring the output from sensors and surveillance cameras. The system can provide alert functions that are activated when an anomaly is detected, and for some types of anomalies the system can use historical data to help discriminating false alarms from actual incidents.

IV. Port Security System

The Port Security System developed in SUPPORT is intended as a tool that can help the PFSO (Port Facility Security Officer) keep track of the risk level for the port in question. The work of the PFSO comprises the following phases:

1) **Planning**
   Identification (and documentation) of threats, Risk Analysis, Identification (and documentation) of Risk Control Measures, Cost-benefit assessment of Risk Control Measures, Recommendations for decision making, Design and documentation of a Security Management Plan.
2) **Day to day Operations**
   Making sure that day to day operations are compliant with the Security Management Plan, Reporting of deviations from the Security Management Plan, Secure proper responses to identified initiating events and actual security incidents, Reporting of security incidents.
3) **Evaluation**
   Validate compliance with Security Management Plan and suggest measures to secure/enhance compliance (such as training, increased awareness, etc.), Validate the efficiency of the Security Management Plan.
4) **Act on basis of the evaluation**
   Initiate actions to secure a better compliance with the Security Management Plan, Initiate actions to secure a more efficient Security Management Plan.

The Port Security System should be able to provide support for all the above mentioned phases.

Today, data from various surveillance sensors (CCTV, access control, etc) are usually processed independently and alarms are raised if something abnormal is detected in either one of the systems as shown in Figure 4. The SUPPORT Port Security System will show how fusion of information from

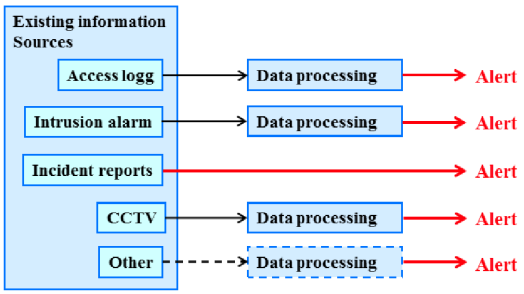

Fig. 4. A common setup for today's port security systems. Different surveillance systems are not integrated with each others and the false alarm rate is high.

different surveillance systems and information systems lead to a lower rate of false positive alarms and over-all better security in ports.

The goal ot the Port Security System is to use available sensor resources as efficiently as possible by setting up a system that helps an operator to create and maintain situation awareness and an understanding of events in the harbor. An important aspect in the design of the Port Security System is that the sensor systems generally create more data than a single operator can handle. In addition, a large amount of information from other systems must also be considered. Examples of such additional information are logs from the access monitoring system, AIS data, administrative data on ships, information on cargo and passengers (for instance from customs), weather information and intelligence from both open and closed sources. In order to support the operator in dealing with all this information, the information sources must be connected in a common information system. In addition, the information system needs to possess some level of machine intelligence which enables it to automatically carry out information processing of routine nature. The automation consists mainly of signal processing of various types of sensor data, such as algorithms for automatic detection of abnormal behavior of persons and vehicles in a video stream. In the SUPPORT solution, so called *events* will be extracted from the processed surveillance data. These events will be fused and an alarm will be raised only if the estimated risk is sufficiently high, *i.e.*, either if different sensors/systems show supporting evidence that something abnormal is happening or if there is an indication - however weak - of events that could potentially lead to the realization of a high-risk, severe-consequence critical event.

The SUPPORT Port Security System is based on Impactorium, a tool for high level information fusion which is developed by FOI and has been described in several publications [9], [10], [8], [11]. Impactorium will be connected to a data base in which processed information originating from sensors, cameras, incident reports and other information sources is stored. Using this information, Impactorium will be able to continuously update its estimated risk level for a number of pre-defined (and pre-modeled) threats. A schematic view of the system is shown in Figure 5.

A prerequisite for the high-level data fusion and formal reasoning done by Impactorium is that input data has a uniform representation. The way to achieve this is to semantically tag the output from different information sources with terms taken from a pre-defined ontology. The taxonomy presented in this paper provides the basis for the ontology that will be used in the Port Security System.

A consequence of using semantically tagged data is also that the system becomes very flexible with regard to installed sensors and sub-system. Instead of having hard-coded relations between different sensors and processing events, higher-level processing functions will ask for available data that have the correct tags and collect it regardless of source. Independence of specific sensor systems is a key property in the SUPPORT Port Security System as it must be possible install, with only minor modifications, in ports of varying types and sizes and with different data generating systems (sensors, surveillance systems, etc.).

V. Port Security Threat Taxonomy

In the previous sections we have explained how the Port Security Threat Taxonomy will be used in the Port Security System. In this section we describe how the taxonomy was constructed and present some excerpts from the end result.

Obviously, all ports are different, and it is not possible to construct a completely generic taxonomy that covers all needs. What we have done in this work is to construct taxonomy templates. We have identified classes of terms that will need to be part of the Port Security Threat Taxonomy, and using the methods described in Subsection V-B we have collected a data set comprising over 300 terms, which have been categorized and inserted in the template. In the taxonomy, the entries are ordered hierarchically in sub-categories, as will be seen in Subsection V-C. Additional structure, such as more complex relations betweens the terms, will be added in the Port Security Ontology. In this paper we present only the domain specific part of the taxonomy. The taxonomy will also need to include some more generic parts that define for example people and animals.

The terms added to the taxonomy have been verified as relevant by both port stakeholders representing the ports participating in the project and the technical experts working on the Port Security System but, the taxonomy is by no means complete. For instance, when configuring the Port Security System to a specific sport, it is likely that one would want to include terms that are more directly related to the system at hand. Also, it must be kept in mind that the world is ever-changing, the antagonists are ever-changing and a system for dealing with threats must therefore be ever-changing to reflect this. The intent is that the constructed taxonomy should be possible to use as a template to which terms can be added and/or removed depending on the needs in a specific port. The approach will be demonstrated within the SUPPORT project, as the taxonomy will be adapted to the setup that will be used in a system demonstration that is scheduled to take place in the port of Gothenburg in 2014.

A. Requirements

The main purpose of the Port Security Threat Taxonomy is to provide the basis for the Port Security Threat Ontology that in its turn will be used by the text based reasoning system

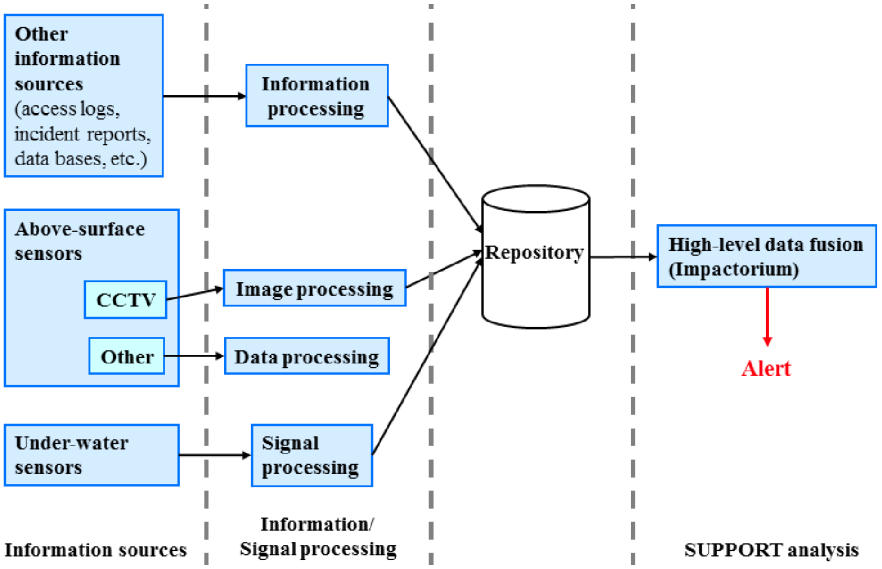

Fig. 5. High-level information fusion makes it possible to reduce the false alarm rate in a port security system.

that constitutes the core of the Port Security System. Thus, the basic requirement on the taxonomy is that it should provide the terms needed to reason about indicators and threats in a port domain. For instance, the taxonomy needs to contain a set of terms that can be used to denote (”tag”) events that could take place within the port area and that might, from a security aspect, be relevant to reason about.

The taxonomy should also support the planning and setup phase of the Port Security System. For this purpose a list of different sensors and information systems should be included in the taxonomy. Once the Port Security System is up and running in a port it should be independent of the individual sensors and information systems used. However, in the setup phase, *i.e.*, when the system is being configured to a specific port facility, it is necessary to manually go through the available information sources and determine what indicators they can detect. In this process, a structured record of different types of information sources and their relations to different indicators can be of use. The reason this mapping between sensors and indicators has to be done manually and for each port is that one must take into consideration not only the nature of the sensors output, but also case-specific circumstances that affect a sensors ability to detect a given indicator. For instance, the output from a security camera could in a general case be used to detect events such as for example person breaking an entry, but with knowledge about the sensors placement, orientation and range the sensor could also be used to associate an event with a specific location.

In addition to its primary functions, the Port Security Threat Taxonomy can be used to facilitate communication between port stakeholders, technical experts, authorities, etc. It can therefore be appropriate to include domain specific terms of more general interest in the taxonomy as well, although it has not been done in the work presented in this paper.

B. *Construction of the taxonomy*

To start with, an outline for the taxonomy was produced based on the expected needs of the Port Security System. Three categories of terms were immediately identified as crucial, namely *Threats*, *Information sources* and *Indicators*. Based on these categories, a first draft of the taxonomy could be produced. As described below, the first draft was constructed mainly using input from project documents describing the port domain and various aspects of the security work in that domain.

Category: Threat In the initial phase of the project, a list of relevant threats and loss events to be considered in the project was produced. These threats were included in the taxonomy after they had been organized into different categories.

Category: Information sources This category was divided into two sub-categories; *Sensors* and *Other information systems*, where *Other information sources* for example included available data bases and manually created incident reports.

Category: Indicators In the high-level reasoning system, an indicator can either be a single detection/observation or a complex event. Regardless of which, the phenomenon must be labelled with a tag that is known to the system before it can be used in the reasoning process. In other words, the tags must be part of the taxonomy. When constructing a list of appropriate tags, it was found useful to consider:

- Circumstances that could lead to realization of the threat
- Conditions that have to be fulfilled in order for the threat to realize
- Events that could mean that the threat is about to be realized

Also, many relevant terms, as well as the relations between them, were found in analysis of the Bow-Tie models of the relevant threats.

Once a first draft of the taxonomy existed, input from port stakeholders and technical experts was retrieved by distribution of questionnaires. Feedback and input were continuously incorporated in the taxonomy. During this process, new categories were added to the taxonomy and existing categories were altered according to the needs that were discovered. After several iterations, the taxonomy was sent out for a final review among members of the project workgroup before it was distributed to other workgroups within the project. Excerpts from the taxonomy can be seen in Subsection V-C.

To summarize, the main sources used to find terms to include in the taxonomy have been:

- Project reports and documentation
- Port stakeholders and security personnel from the companies and organizations participating in the project
- Technical experts working on the Port Security System
- Experts on sensors and signal processing

C. Components of the taxonomy

In the final version of the Port Security Threat Taxonomy the terms are divided into ten main categories:

1) Threats/Loss events
2) Targets
3) Sensors
4) Sensor/Information systems
5) Other information sources
6) Indicators/events
7) Locations
8) Means of transportation
9) Weapons and CBRN
10) Event/activity tags

Excerpts from three of the categories, *Sensors*, *Indicators/events* and *Locations* can be seen in Tables I, II and III, respectively.

To conclude, we once again point out that the constructed taxonomy should be seen as a template. It will need to be adapted and refined before it can be used in a specific application, and after adaptation it will need to be continuously evaluated and updated based on updated risk assessments and actual effectiveness/performance.

VI. Conclusion

In this paper we have described the construction of a taxonomy that will be used in the decision support system of the EU FP-7 project SUPPORT (Security UPgrade for PORTs). The primary function of the SUPPORT decision support tool is to assist a human operator in the assessment of threat levels for a number of pre-defined threats. More precisely, the system uses text based automatic reasoning and high-level information fusion to identify threat indicators in the input data. Thus, the existence of a taxonomy containing well-defined terms that can be used by the reasoning system is essential.

In the paper we described the method used to construct the taxonomy, involving the construction of a draft taxonomy and gathering of information using questionnaires. The questionnaires were motivated by the necessity to embody experience and knowledge from different groups of people involved in the

TABLE I. Taxonomy: Sensors (excerpt from full sensor taxonomy)

underwater sensor	Active sonar	
	Acoustic sensor/hydrophone	
	Sensor arrays	Acoustic sensors
		Electrodes
		Magnetometers
Visible light image sensor		
	Surveillance camera (CCTV)	
	Digital photography	
	IP camera	
Radar	See-through-the-wall radar	
	Real aperture radar (RAR)	
	Synthetic aperture radar (SAR)	
	TeraHertz-radar (microwave radar)	
Motion detectors		
Door/window alarms		
IR-sensors	Imaging IR-sensor	
	Passive (non-imaging) IR-sensor	
	Active IR-sensor (photo beam)	

TABLE II. Taxonomy: Events tags (excerpt from full event taxonomy)

Events detected in port or close to port area	Rowdy person/group of people
	Passenger bypasses passport/visa control
	Person/group of people at unexpected time/place
	Car/truck parked or driving at unexpected time/place
	Vessel moored or driving at unexpected time/place
	Detection of weapon/fire/poisonous subject/radioactivity/explosives/hidden people
	Infrastructure/roads/waterways are blocked
	Person/persons are breaking an entry (climbing a fence, running a car through a wall, breaking a window, forcing a door open, ...)
	People/divers/small boats in the water
Events outside port area and vicinity	Act of terrorism in country, region, city, or other port
	Law enforcement notification for increased security risk in the country, region or city
	Vessel in 10 previous ports at least twice raised ISPS Security levels
	Vessel comes from country with weak public administration, high security threat level, rebellion etc.

TABLE III. TAXONOMY: LOCATIONS (EXCERPT FROM FULL EVENT TAXONOMY)

Passenger terminals	Vehicle area	Entrance gates
		Waiting area
	Walking passengers	Entrance gates
		Waiting area
	Administrative building	
Gas terminal	Entrance gates	
	Quay area (loading and unloading of goods)	
	Yard/Storage area	
Oil terminal	Entrance gates	
	Quay area (loading and unloading of goods)	
	Yard/Storage area	
Container Terminals	Entrance gates	
	Quay area (loading and unloading of goods)	
	Yard/Storage area	
Liquid Bulk Terminals	Entrance gates	
	Quay area (loading and unloading of goods)	
	Yard/Storage area	
Warehouses/storage areas	Outdoor storage area	
	Warehouses	

project, most of which are not used to formally defining their vocabulary. Over-all, the method proved to work well and gave the expected output.

ACKNOWLEDGMENT

This research was funded by the European Commission under Grant Agreement number 242112 (SUPPORT), by the R&D programme of the Swedish Armed Forces and by Vinnova through the VINNMER programme.

REFERENCES

[1] The SUPPORT project http://www.supportproject.info/ (accessed 2013-04-15)

[2] M.M. Kokar, C.J. Matheus, and K. Baclawski, *Ontology-based situation awareness*, Information Fusion, volume 10, issue 1, 2009.

[3] (MSC 83/INF.2) FORMAL SAFETY ASSESSMENT, Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process (MSC/Circ.1023MEPC/Circ.392). IMO Maritime Safety Committee 83rd session, Agenda item 21, May 14th, 2007.

[4] V.M. Trbojevic, and B.J. Carr, *Risk based methodology for safety improvements in ports*, Journal of Hazardous Materials, volume 71, issues 13, 2000.

[5] C.W. Holsapple and A.B. Whinston, *Decision Support Systems: A Knowledge-Based Approach*, West Publishing Company, 1996.

[6] D.J. Power, and R. Sharda, *Decision Support Systems*, Springer Handbook of Automation (S.Y. Nof, Ed.), Springer Berlin Heidelberg, pp. 1539-1548, 2009.

[7] M.R. Endsley, *Measurement of Situation Awareness in Dynamic Systems*, Human factors, 37(1), 65-84, 1995.

[8] J. Brynielsson, A. Horndahl, L. Kaati, C. Mårtenson, and P. Svenson, "Development of Computerized Support Tools for Intelligence Work", in *Proceedings of the 14th International Command and Control Research and Technology Symposium (14th ICCRTS)*, Washington, District of Columbia 2009.

[9] P. Svenson, T. Berg, P. Hörling, M. Malm, and C. Mårtenson, "Using the impact matrix for predictive situational awareness", in *International Conference on Information Fusion*, 2007.

[10] R. Forsgren, L. Kaati, C. Mårtenson, P. Svenson, and E. Tjörnhammar, "An overview of the Impactorium tools", in *Proceedings of SWIFT2008*, 2008.

[11] P. Svenson, R. Forsgren, B. Kylesten, P. Berggren, W.R Fah, M.S. Choo, and J. Hann, "Swedish-Singapore studies of Bayesian Modelling techniques for tactical Intelligence analysis", in *Proccedings of the 13th International Conference on Information Fusion*, 2010.