



Article

CoRiMaS—An Ontological Approach to Cooperative Risk Management in Seaports

Salvatore F. Pileggi ¹, Marius Indorf ², Ayman Nagi ^{2,*} and Wolfgang Kersten ²

¹ School of Information, Systems and Modelling, University of Technology Sydney, Sydney, NSW 2007, Australia; SalvatoreFlavio.Pileggi@uts.edu.au

² Institute of Business Logistics and General Management, Hamburg University of Technology, 21073 Hamburg, Germany; Marius.Indorf@tuhh.de (M.I.); W.Kersten@tuhh.de (W.K.)

* Correspondence: Ayman.Nagi@tuhh.de

Received: 13 May 2020; Accepted: 7 June 2020; Published: 11 June 2020



Abstract: For today's global value chains, seaports and their operations are indispensable components. In many cases, the cargo handling takes place in close proximity to residential and/or environmentally sensitive areas. Furthermore, seaports are often not operated by a single organization, but need to be considered as communities of sometimes hundreds of internal and external stakeholders. Due to their close cooperation in the cargo handling process, risk management should be a common approach among the internal stakeholders as well in order to effectively mitigate and respond to emerging risks. However, empirical research has revealed that risk management is often limited to the organization itself, which indicates a clear lack of cooperation. Primary reasons in this regard are missing knowledge about the relations and responsibilities within the port and differing terminologies. Therefore, we propose an ontology (CoRiMaS) that implements a developed reference model for risk management that explicitly aims at seaports with a cooperative approach to risk management. CoRiMaS has been designed looking at the Semantic Web and at the Linked Data model to provide a common interoperable vocabulary in the target domain. The key concepts of our ontology comprise the hazard, stakeholder, seaport, cooperation aspect, and risk management process. We validated our ontology by applying it in a case study format to the Port of Hamburg (Germany). The CoRiMaS ontology can be widely applied to foster cooperation within and among seaports. We believe that such an ontological approach has the potential to improve current risk management practices and, thereby, to increase the resilience of operations, as well as the protection of sensitive surrounding areas.

Keywords: cooperation; ontology; risk management; seaport

1. Introduction

Seaports are important logistical nodes for global trade. In 2018 only, a total of 11,002 million tons of goods were loaded for international seaborne trade, including crude oil, petroleum products, gas, main bulks, such as iron ore, grain, and coal, as well as other dry cargo [1]. This amount of goods handled has been increasing constantly throughout the last decades. Consequently, seaports play an essential role in the logistical chain, as all seaborne trade has to pass through their facilities, where the transport mode is changed from a water to a land based one (or vice versa). Seaports are often located in densely populated areas, meaning that dangerous and non-dangerous goods are loaded and unloaded in close proximity to sensitive urban environments. In Germany for instance, according to the Federal Office of Statistics, 44.5 million tons have been transported by sea and 47.3 million tons on inland waterways in 2017 [2]. These volumes are handled at ports and represent combined about 31% of the total amount of dangerous goods transported.

Risk management, including its proactive and reactive measures, is vital for ensuring safe and secure operations within the seaports. This was demonstrated, for example, by an incident on board of the “CCNI AURACO”, a mega container ship, which caught fire in 2016 after an explosion at the dock at the Port of Hamburg, Germany. During welding work onboard the ship, a container exploded and the fire spread to nearby units, causing thick smoke covering both the vessel and terminal. As the crew was not able to extinguish the flames, they had to request assistance from local authorities. The fire extinguishing process involved 150 firefighters, several machines, and extensive equipment [3]. In total, it took the emergency response team almost four days to eliminate the threat as the temperature inside the ship was extremely high, causing severe damage to the ship’s stability (Fire on Container Ship CCNI Arauco Was Extinguished—Maritime Herald [Online], <http://www.maritimeherald.com/2016/fire-on-container-ship-ccni-arauco-was-extinguished/>. Accessed: 8 January 2019) and disrupting operations at the terminal for significant time. Even after the fire services completed their work, the affected berths remained closed due to police investigation and clean-up work (Burchardkai: Fire on “CCNI Arauco” Extinguished—HHLA [Online], <https://hhl.de/en/2016/09/burchardkai-fire-on-ccni-arauco-extinguished.html>. Accessed: 8 January 2019). The incident so severe that emergency services personnel from other cities had to be requested by the local authorities in Hamburg in order to get the critical situation under control (Photos: Container Ship in Hamburg Harbor Still Burns—The Maritime Executive [Online], <https://www.maritime-executive.com>. Accessed: 8 January 2019).

The case described is only one example of many and of the possible risks that could endanger lives, environment, infrastructure as well as operations within and round the seaport. According to the European Maritime Safety Agency [4], about 50% of all marine casualties and incidents took place in ports or their nearby areas (see Figure 1). In 2017 alone, more than 1700 events were registered in European port areas or involving European ships in port areas overseas. The data reported in the figure also indicates that from 2011 to 2014, the total amount of casualties and incidents has risen. That high level has not decreased ever since. During this period, the proportion of events in ports and their nearby areas has also increased to about half of the total. Considering this development, ports and their immediate surroundings are—compared to coastal waters, the open sea, and inland waters—affected most frequently and require, therefore, special attention in order to improve safety and security.

In addition, the case shows that usually many parties or stakeholders in a seaport have to be involved in the process of risk management in order to reduce the occurrence probability and impact severity in an effective manner. Establishing a thorough risk management in a seaport requires, hence, an extensive and reliable cooperation between many organizations.

Even though risk management is gaining a greater importance and is receiving increasing attention in seaports, standard procedures that are universally applicable do not exist. In fact, risk management activities are currently very port and stakeholder specific [5]. This also represents a great barrier for cooperative activities in risk management, which are necessary in order to mitigate the effects of hazards and resulting risks as demonstrated by the above reported CCNI AURACO incident. It is, therefore, our first objective to design a suitable model for cooperative risk management that helps practitioners and researchers to develop a common understanding, how risk management among independent organizations should be carried out.

In order to have our model working in practice within and among the diverse organizations, we provide an ontology [6], understood like a formal conceptualization of a domain, to allow (i) the effective description and re-use of risk management activities and environments; (ii) the analysis of current strategies for specific risks across relevant stakeholders; as well as (iii) their evolution, alignment, and optimization. In addition, the ontology will enable comparisons among different seaports, for example with respect to the applied methods or stakeholder structure. In general, the formalization is expected to define a risk management framework within and across seaports.

The considered categories, attributes, and relations strive to reduce the complexity and to organize the different concepts of risk management in seaports in a suitable way, such that the process is

supported and its practicability increased. The developed framework is generic in nature and may be applied to any seaport as well as used by any organization willing to leverage its risk management activities, shaping the overall risk landscape positively.

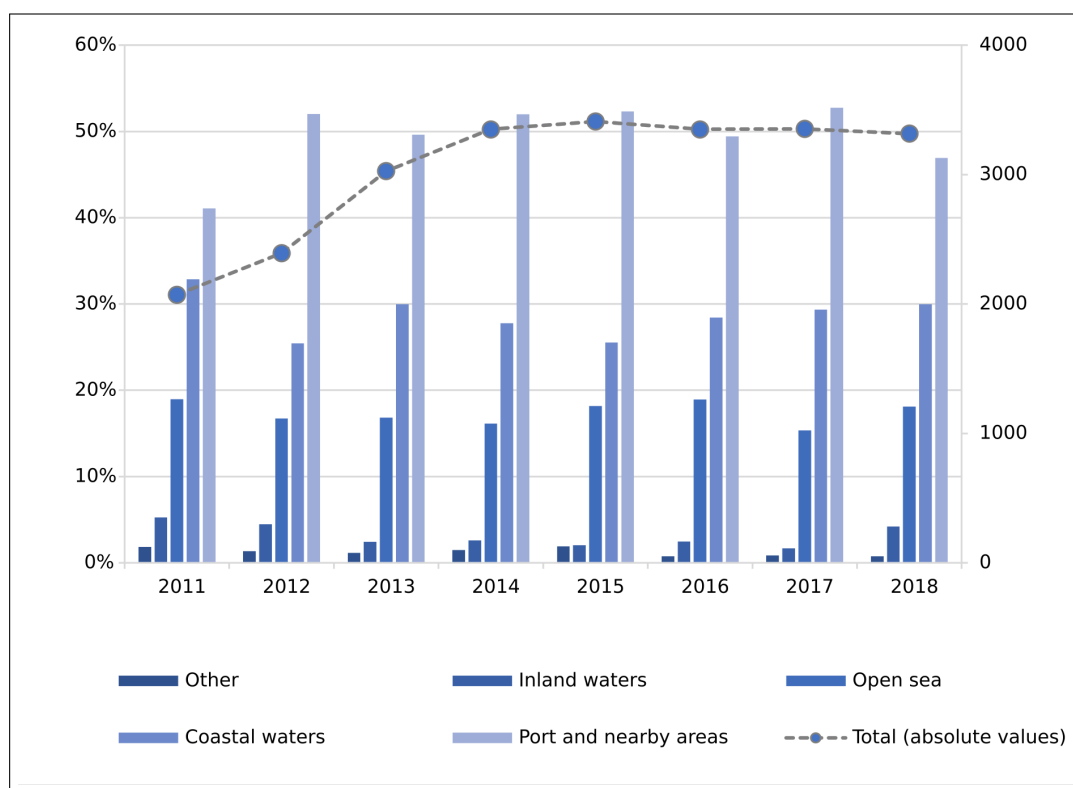


Figure 1. Distribution of marine casualties and incidents by location.

1.1. An Ontological Approach to Establish a Common Language for Cooperative Risk Management

The benefits introduced by the adoption of ontologies have been extensively discussed in literature, in general terms [6] or in the context of specific application domains (e.g., recently in Software Engineering [7]).

Those advantages can be summarized in the following points:

- *Formal Specifications and Analysis.* Ontology allows a formal unambiguous specification of a given conceptualization [8]. That is a basic but critical feature as, if properly adopted, ontology may limit the risk of misinterpretation. At the same time, a formal conceptualization provides an ideal analysis framework [6].
- *Interoperability, Integration, Re-use, and Portability.* Assuming computational ontologies [8] implemented in a standard language, the resulting data model becomes a kind of potentially interoperable data structure that enables data integration and re-use as many studies (e.g., [9]) clearly show.
- *SW-enabled data infrastructure.* If ontologies are developed upon Semantic Web technology, then they are intrinsically enabled in the Semantic Web [10]. It allows for an effective implementation of Linked Data philosophy [11], as well as a global understanding of knowledge bases facilitated by an improved interoperability model (known as Semantic Interoperability [12]).
- *Inference and Automatic Reasoning.* Ontology assumes knowledge at different levels. Indeed, grounded knowledge is defined by explicit “statements”, while inference rules and structures provides a further level of knowledge. As inference rules and structures are also defined by adopting standard languages and they are part of ontologies, the inference process, commonly known as reasoning, is implemented by standard components (reasoners). It results in standard

automatic reasoning, as different independent systems interpret a given ontology in the same way. Automatic reasoning is a key feature within knowledge-based systems. For instance, in the context of this work, inference may support processes for consistency checking.

Informally, rather than a prescriptive approach, ontology provides a “common language” that can be dynamically extended and linked to others. Our previous work (Current Status of Risk Management Process at Major Baltic Sea Region Seaports: An Interview Study, <https://blogit.utu.fi/hazard/publications/>) has clearly shown that the missing “common language” is a major obstacle for cooperative risk management in seaports today. As discussed later on in the paper, our ontology expresses high-level semantics. Therefore, such a language is directly usable by end-users. At the same time, the ontology is developed upon Semantic Web Technology, so it is machine-interpretable.

1.2. Structure of the Paper

In Section 2, we discuss works related to this research. The analysis predominantly focuses on the current state of risk management in seaports and on existing models for risk management. Then, in Section 3, we introduce the reference model (CoRiMaS) developed for cooperative risk management in seaports. The model visualizes informally key relations among the organizations and their surroundings within the field studied. On the one hand, the intention is to also allow non-experts to understand the dynamics and motives in risk management; on the other hand, the model lays out the foundation for the ontology developed in the subsequent section. Section 4 deals with the description of the proposed ontology. Section 5 includes the case study of the Port of Hamburg, being the third largest seaport in Europe. The full description of the Port of Hamburg from a risk management perspective is out of the scope of the paper and, indeed, only a very minor subset of concepts is reported. Section 6 provides a brief overview of different possible ways to use the ontology in practice. The paper ends with a conclusion section in which future work is briefly discussed too.

2. Related Work

In this section, we provide a concise analysis and a brief discussion of existing works. As an exhaustive overview of solutions, issues, and challenges related to generic risk management is out of the scope of the paper, we focus uniquely on seaports (Section 2.1). Additionally, we present, in short, a review of ontology-based solutions to risk management (Section 2.2).

2.1. Risk Management and Seaports

Due to the vast amount of hazards and risk sources in seaports, an efficient and effective risk management is gaining further importance [13]. The research on risk management in seaports has a wide scope and covers several different aspects such as risk factors [14–17], risk assessment [18–22], natural hazards [23–25], management of disruptions [26], disaster response planning [27], empirical data [28], and frameworks [29].

In some cases (i.e., [14,19]), the contributing authors develop very specific approaches only applicable to particular ports. In most cases, however, the concepts and methods proposed are quite generic and may be applied to different types of (sea)ports.

In a recent co-citation analysis, the current state of risk management research in seaports was examined [5]. The authors identified eight clusters based on a structured approach. The study revealed that there is a clear gap concerning cooperative risk management in seaports with no developed theoretical or empirical models. The current research focuses on approaches and studies for analysis and decision-making, as well as studies related to the impacts of natural hazards on coastal and port areas. Minor research areas, such as assessment methods for hazardous spills, ballast water, and liquefied natural gas (LNG) were also identified.

As organizations are closely interwoven in their operations and are located in close proximity to each other, the area of cooperative risk management is of a particular importance. Only if proactive

and reactive activities are well aligned and knowledge is shared among the relevant organizations, can a thorough risk management process be guaranteed. This research aims to address the above mentioned gap by applying an ontology-based approach. We believe that it can be an additional value for the quality risk management in complex systems because, by providing a descriptive formal conceptualization of the target domain, such an approach may integrate existing strategies and methods to facilitate an unambiguous use of the framework within computer systems in a context of interoperability.

2.2. Ontology for Risk Management

Ontologies are extensively used within the risk management domain and, indeed, a number of contributions may be easily identified in literature. They often refer to relatively generic applications, such as improving risk analysis [30] and supporting risk management processes [31]. Other contributions address much more specific sub-domains, i.e., risk management in construction projects [32] and information security [33]. Many solutions deal with specific problems, for instance job hazard analysis [34] and scenario-based evaluation [35] and risk management in small-medium sized enterprises [36]. Often ontology-based systems focus on a given hazard category, such as geographical hazards [37].

The ontology proposed implements our reference model for risk management which explicitly aims at seaports with a collaborative approach to risk management. Semantic technology allows the alignment with other ontologies in the domain of risk management, as well as with upper vocabularies to establish an integrated knowledge environment.

3. CoRiMaS: A Reference Model to Risk Management in Seaports

In general, a *seaport* can be defined as “the place of the change of means of transport from inland into a water bound one” [38] as well as the place of the transshipment from ship to ship. Seaports thereby represent very important logistical nodes for many industries. Due to this importance, smooth and safe operations without severe emergencies and accidents are in the interest of all organizations that are linked directly or indirectly to the seaport. Furthermore, seaports are often located near, or even in, densely populated areas and natural habitats that must be protected and preserved. A proper risk management within and across the involved organizations is the key to achieve these objectives. In particular, the cooperative component is a challenge for many actors in a seaport but nonetheless a substantial part of a preventive and reactive risk management that needs to be further enhanced.

The reference model—CoRiMaS—developed for cooperative risk management is shown in Figure 2. It helps to generate a common, yet informal, understanding of this complex matter.

In such a model, *risk* and *hazard* are closely linked to each other. Hazard can represent any physical or chemical condition that has the potential to cause a damage to people, property, or the environment [39]. An example of a hazard is a pressurized tank containing a large quantity of ammonia. Hazards can be classified from several perspectives. According to their origin, hazards can be divided into natural and man-made hazards [40]. Natural hazards are adverse events that arise from the occurring processes, which exist in the natural environment such as floods or earthquakes. Man-made hazards represent any intentional or non-intentional actions caused by humans that have the potential to cause damage to others or physical infrastructure.

The different hazard and/or types influence the assessment process of the potential risks that could arise. The core dimensions that characterize a particular risk are its occurrence probability and its consequence. *Risk occurrence probability* quantifies the likelihood of occurrence of a specific event that is caused by a potential hazard [39]. *Risk consequence* measures the severity or expected effects an event’s outcome can have [39]. For instance, an ammonia cloud travelling at a certain velocity and direction is likely to injure a definite number of people. A data collection process is required to make a better estimation of the risk occurrence probability and risk consequence. For instance, the estimation

can be based on the amount of ammonia released in kilogram per second and the wind speed in kilometres per hour.

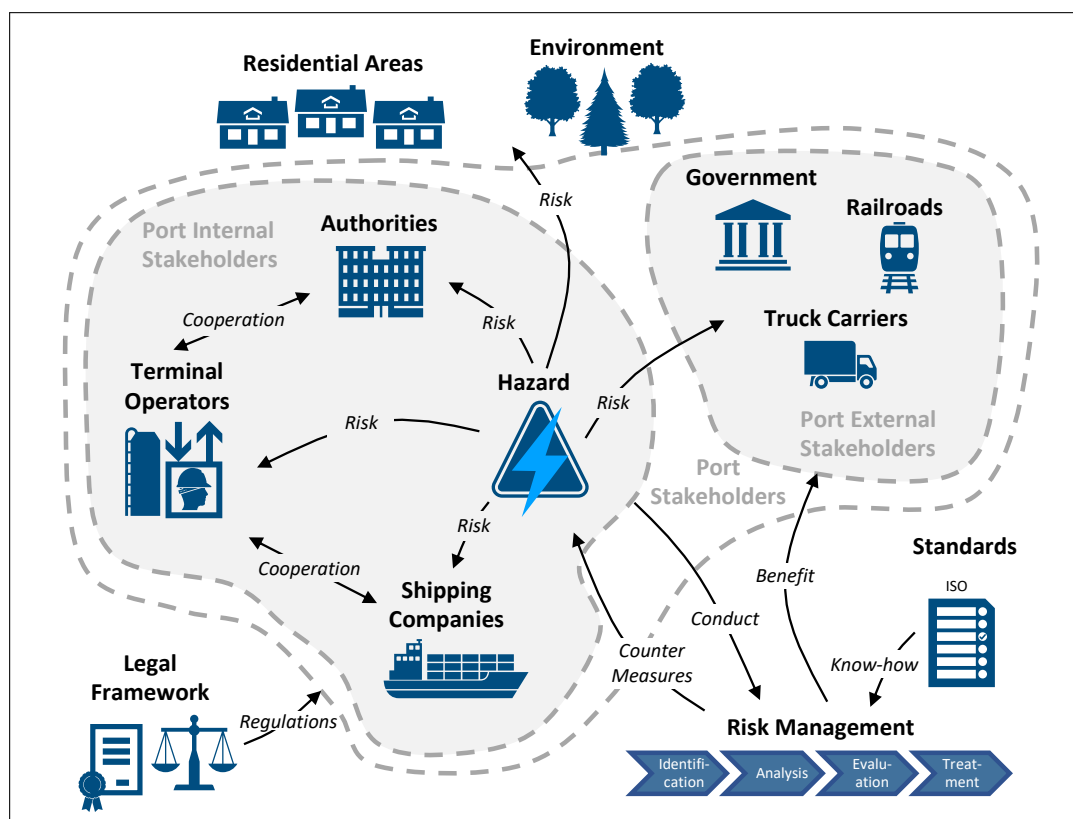


Figure 2. Reference model for cooperative risk management in seaports (CoRiMaS).

As mentioned before, a seaport is a complex community of several internal and external stakeholders [41,42] that could be affected, directly or indirectly, by the risks resulting from man-made or natural hazards. Since the stakeholders are often located in close proximity and premises are frequently adjacent to each other, the importance of smooth and safe operations in the seaport as a whole is further underlined. Consequently, it is inevitable to cooperate with other organizations with respect to risk management and the counter measures adopted hereby. The legal framework defines the regulations that the actors in a seaport are obliged to follow. In some cases, these regulations even demand appropriate actions to prevent or respond to risks.

In general, a process can be defined as a “set of interrelated or interacting activities that use inputs to deliver an intended result” (Quality management systems, EN ISO 9000:2005, 2005). In case of the risk management process, these activities can be grouped into sequential phases of identifying, analysing, evaluating, and treating different types of risks. How these phases are executed in detail, is documented in standards, such as the ISO 31000 (Risk Management, ISO 31000:2009(E), 2009) or the AS/NZS 4360:2004 [43]. In a seaport, the internal stakeholders conduct risk management activities and the external stakeholders benefit from the adopted counter measures, as the consequences of the overall risk landscape are mitigated.

A method in risk management can be qualitative, semi-quantitative, or quantitative. These methods can be applied in either one or multiple phases of the risk management process. As qualitative methods are simpler but more subjective, quantitative methods are more objective but require substantial data and analysis. Semi-quantitative methods combine the aspects of quantitative and qualitative approaches. A countermeasure is necessary to reduce the occurrence probability and/or consequences of the corresponding risk [43].

4. CoRiMaS Ontology

As previously introduced, this section focuses on a formal specification of the proposed cooperative model by adopting Semantic Web technology as per W3C (World Wide Web Consortium—<https://www.w3.org>) standards. This formal specification is used to convert the informal model into a set of classes, relationships, and attributes defined according to a standard ontology language. It allows for the unambiguous use of the framework in practice, as well as enabling the resulting data structure within computer systems.

CoRiMaS ontology was designed by looking at the Semantic Web [10] and at the Linked Data model [11]. It was developed upon semantic technology (Ontology Web Language—OWL 2 [44]) with the support of Protege [45]. The ontology is freely available under the Creative Commons Attribution 4.0 International License. Main classes, object, and data properties are listed in Tables 1–4, respectively.

We checked the consistency of the ontology within Protege by using inference engines available in such an environment, i.e., HermiT [46]. We also performed the same process outside Protege; for instance, the ontology may be visualized by WebVOWL [47], which implements VOWL [48] and builds ontological visualizations by processing Resource Description Framework Schema (RDF-S) [49] inference rules, including *rdfs:domain/rdfs:range* extensively adopted in our implementation. We do not specify the type of the attributes in our visualizations. We refer to them generically as “literals”, according to the typical terminology adopted within the Semantic Web community. Last but not least, the ontology was tested within the knowledge-based system currently under development at the University of Technology, Sydney. This environment is based on Pellet [50] and uses ARQ [51] as a SPARQL (<https://www.w3.org/TR/sparql11-query/>) wrapper to support query functionalities.

A core set of internal concepts, representing the underlining model, is depicted in Figure 3. This diagram provides a concise overview of the ontology. The diagram adopted for the visual representation is a knowledge graph derived from the language adopted (OWL). The same approach was followed to describe more detailed structures or examples of use in other parts of the paper. According to this simplified view, the target environment is understood as a composition resulting from the specification of seaports and hazards, which are represented by the corresponding ontological concepts (*CoRiMaS:SeaPort* and *CoRiMaS:Hazard*). A seaport is understood and, therefore described, as a virtual organization (*CoRiMaS:VirtualOrganization*) resulting from the coexistence of several different stakeholders (*CoRiMas:Stakeholder*) and their interactions. The key concept, which connects the different aspects of the model all together is the co-operation aspect (*CoRiMaS:CooperationAspect* in the ontology) that involves stakeholders in a given risk management process (*CoRiMaS:Process*).

CoRiMaS ontology provides a number of hierarchically organised classes. They represent the types that the different concepts may be associated with. This structure is extensible by definition, so new types may be provided, and can also be merged with classes from other vocabularies. However, depending on the context, on the target system, and on the kind of user, providing new classes can lead to some issues, including unmanaged duplications, inconsistencies, and overlapping. In order to allow a dynamic extension of taxonomies without the need to define new classes, the ontology enables the specification of types as instances (OWL individuals) of generic class types that are eventually associated with the target concept. Examples are provided in the next section.

Table 1. Main classes description.

Class	Description
<i>Hazard</i>	A chemical or physical condition that has the potential for causing damage to people, to property, or to the environment [39].
<i>Risk</i>	A measure of human injury, environmental damage or economic loss in terms of both the incident likelihood and the magnitude of the loss or injury [39].
<i>Natural_Hazard</i>	Ordinary occurring process which exists in the natural environment [40,52].
<i>Man-made_Hazard</i>	Intentional or unintentional actions that have a potential to cause harm to people or organizations [40].
<i>Stakeholder</i>	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity ^a .
<i>Actor</i>	Synonymous with Stakeholder.
<i>Player</i>	Synonymous with Stakeholder.
<i>Internal_Stakeholder</i>	Stakeholders who directly engage in the various daily activities at the seaport (definition based on [41,53]).
<i>External_Stakeholder</i>	Stakeholders who do not directly engage in the various daily activities at the seaport but are dependent and/or effected by the activities of the seaport's internal stakeholders (definition based on [41,53]).
<i>StakeholderCategory</i>	Category associated with stakeholders.
<i>VirtualOrganization</i>	A network of organizations that share resources and skills to achieve its mission/goal. It is not limited to an alliance of enterprises [54,55].
<i>SeaPort</i>	The place of the change of means of transport from an inland into a water-bound one [38].
<i>PortType</i>	The port type characterizes the port according to different dimensions, such as location or water access.
<i>PortFeature</i>	A port feature indicates a characteristic of the port, such as available terminals or hinterland connections.
<i>PortLocation</i>	It defines the geographical position of a seaport.
<i>Legal_Framework</i>	The legal framework includes all respective national laws and regulations ^d .
<i>CooperationAspect</i>	A particular part or feature of the overall cooperation among stakeholders.
<i>CooperationAspectIntensity</i>	The intensity of the corresponding cooperation aspect, e.g., the intensity of communication between two stakeholders with regards to operational risks.
<i>Process</i>	A set of interrelated or interacting activities that use inputs to deliver an intended result ^b .
<i>ProcessPhase</i>	A distinct period or stage in a series of events or a process of change or development ^c .
<i>PhaseActivity</i>	A phase activity comprises a set of actions that deliver an intended result to the corresponding phase. For instance, in the risk treatment phase, the activity of defining suitable counter measures comprises actions such as organizing workshops or collecting expert estimates.
<i>RM-Method</i>	An elaborated approach that can be used to identify, analyse, evaluate, handle and/or monitor risks [56].
<i>Measure</i>	A counter measure is implemented in the process of risk treatment to modify risk. A counter measure can be either proactive or reactive.
<i>Proactive</i>	Creating or controlling a situation rather than just responding to it after it has happened ^c .
<i>Reactive</i>	Acting in response to a situation rather than creating or controlling it ^c .

^a International Standard ISO 31000:2009(E), S. 4; ^b ISO Standard EN ISO 9000:2005, S. 18; ^c Oxford Dictionary; ^d Wolke (2017)—Risk Management, ISBN: 978-3110440522.

Table 2. Semantic structure of the main classes composing the ontology.

Class	Sub-Class	Disjoint	Equiv.
<i>Hazard</i>	-	-	Risk
<i>Risk</i>	-	-	Hazard
<i>Natural_Hazard</i>	Hazard	Man-made_Hazard	-
<i>Man-made_Hazard</i>	Hazard	Natural_Hazard	-
<i>Stakeholder</i>	-	StakeholderCategory	Actor, Player
<i>Actor</i>	-	-	Stakeholder
<i>Player</i>	-	-	Stakeholder
<i>Internal_Stakeholder</i>	Stakeholder	External_Stakeholder	-
<i>External_Stakeholder</i>	Stakeholder	Internal_Stakeholder	-
<i>StakeholderCategory</i>	-	Stakeholder	-
<i>VirtualOrganization</i>	-	-	-
<i>SeaPort</i>	VirtualOrganization	PortType	-
<i>PortType</i>	-	SeaPort	-
<i>PortFeature</i>	-	-	-
<i>PortLocation</i>	-	-	-
<i>Legal_Framework</i>	-	-	-
<i>CooperationAspect</i>	-	-	-
<i>CooperationAspectIntensity</i>	-	-	-
<i>Process</i>	-	ProcessPhase, PhaseActivity	-
<i>ProcessPhase</i>	-	Process, PhaseActivity	-
<i>PhaseActivity</i>	-	ProcessPhase, Process, RM-Method	-
<i>RM-Method</i>	-	PhaseActivity	-
<i>Measure</i>	-	-	-
<i>Proactive</i>	-	-	-
<i>Reactive</i>	-	-	-

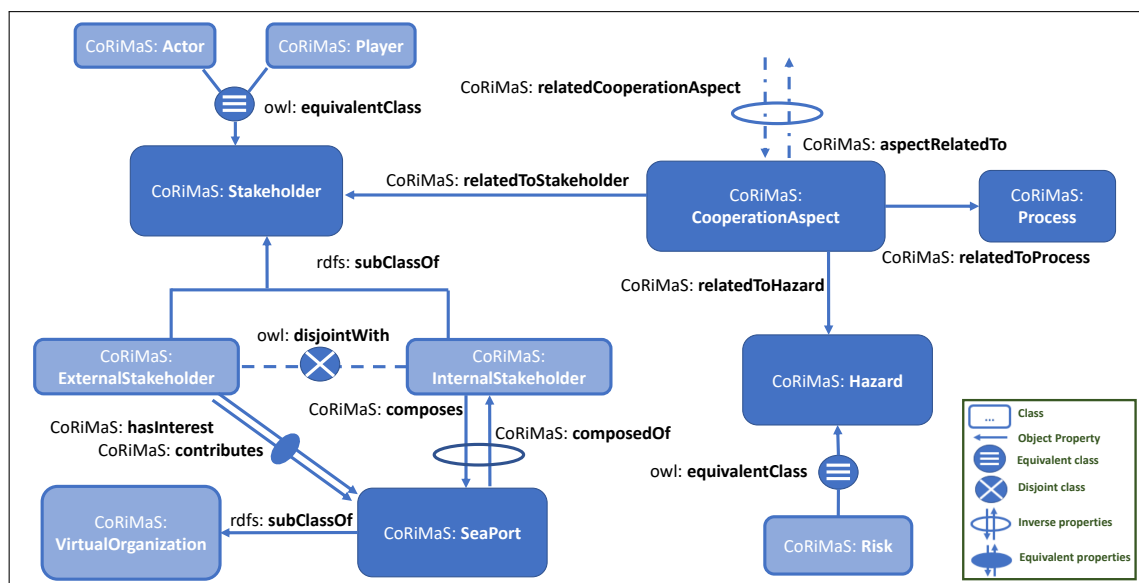


Figure 3. CoRiMaS ontology overview.

Table 3. Main object properties.

Property	Sub-Prop.	Funct.	Equiv.	Inverse	Domain	Range
<i>aspectRelatedTo</i>	-	no	-	relatedToCooperationAspect	CooperationAspect	-
<i>relatedToCooperationAspect</i>	-	no	-	aspectRelatedTo	-	CooperationAspect
<i>relatedToCooperationAspectIntensity</i>	aspectRelatedTo	yes	-	-	CooperationAspect	CooperationAspectIntensity
<i>relatedToHazard</i>	aspectRelatedTo	no	-	-	CooperationAspect	Hazard
<i>relatedToProcess</i>	aspectRelatedTo	yes	-	-	CooperationAspect	Process
<i>relatedToProcessPhase</i>	aspectRelatedTo	no	-	-	CooperationAspect	ProcessPhase
<i>relatedToStakeholder</i>	aspectRelatedTo	no	-	-	CooperationAspect	Stakeholder
<i>has_measure</i>	-	no	-	-	-	Measure
<i>hasFeature</i>	-	no	-	-	SeaPort	PortFeatures
<i>legal_framework</i>	-	no	-	-	SeaPort	Legal_Framework
<i>portProperty</i>	-	no	-	-	-	-
<i>composedOf</i>	portProperty	no	-	composes	Internal_Stakeholder	SeaPort
<i>composes</i>	portProperty	no	-	composedOf	SeaPort	Internal_Stakeholder
<i>contributes</i>	portProperty	no	hasInterest	-	external_Stakeholder	SeaPort
<i>hasInterest</i>	portProperty	no	contributes	-	external_Stakeholder	SeaPort
<i>hasPortLocation</i>	portProperty	no	-	-	SeaPort	PortLocation
<i>hasPortType</i>	portProperty	no	-	-	SeaPort	PortType
<i>hasStakeholderCategory</i>	-	no	-	-	Stakeholder	StakeholderCategory
<i>process_structure</i>	-	no	-	-	-	-
<i>belongs_to_process</i>	process_structure	no	-	composedOf_ProcessPhase	ProcessPhase	Process
<i>composedOf_ProcessPhase</i>	process_structure	no	-	belongs_to_process	Process	ProcessPhase
<i>phase_activity</i>	process_structure	no	-	-	ProcessPhase	PhaseActivity
<i>previous_phase</i>	process_structure	no	-	-	ProcessPhase	ProcessPhase
<i>rm-method</i>	process_structure	no	-	-	ProcessPhase	RM-Method

Table 4. Main data properties.

Property	Sub-Property of	Functional	Domain
<i>risk_property</i>	-	no	Hazard
<i>risk_consequence</i>	<i>risk_property</i>	yes	Hazard
<i>risk_occurrenceProbability</i>	<i>risk_property</i>	yes	Hazard
<i>cooperationAspectIntensity</i>	-	yes	CooperationAspect
<i>portAttribute</i>	-	no	SeaPort
<i>hinterlandConnection</i>	<i>portAttribute</i>	no	SeaPort
<i>portTerminal</i>	<i>portAttribute</i>	no	SeaPort
<i>waterCondition</i>	<i>portAttribute</i>	no	SeaPort
<i>weatherCondition</i>	<i>portAttribute</i>	no	SeaPort

4.1. Hazard

A hazard is specified in CoRiMaS according to the subset of the ontology proposed in Figure 4 by using either the internal concept *CoRiMaS:Hazard* or *CoRiMaS:Risk*. The ontology provides a specific extendible taxonomy to properly classify hazards. The current version is based on the key difference between a natural hazard (*CoRiMaS:Natural_Hazard* in the ontology) and a man-made hazard (corresponding to the internal concept *CoRiMaS:Man-made_Hazard*). As reported in the diagram, a further class break down allows for a fine grained classification. Each hazard may be characterized properly by specifying its attributes (e.g., *CoRiMaS:risk_occurrenceProbability* and *CoRiMaS:risk_consequence*) and related to cooperation aspects through the internal property *CoRiMaS:relatedToHazard*.

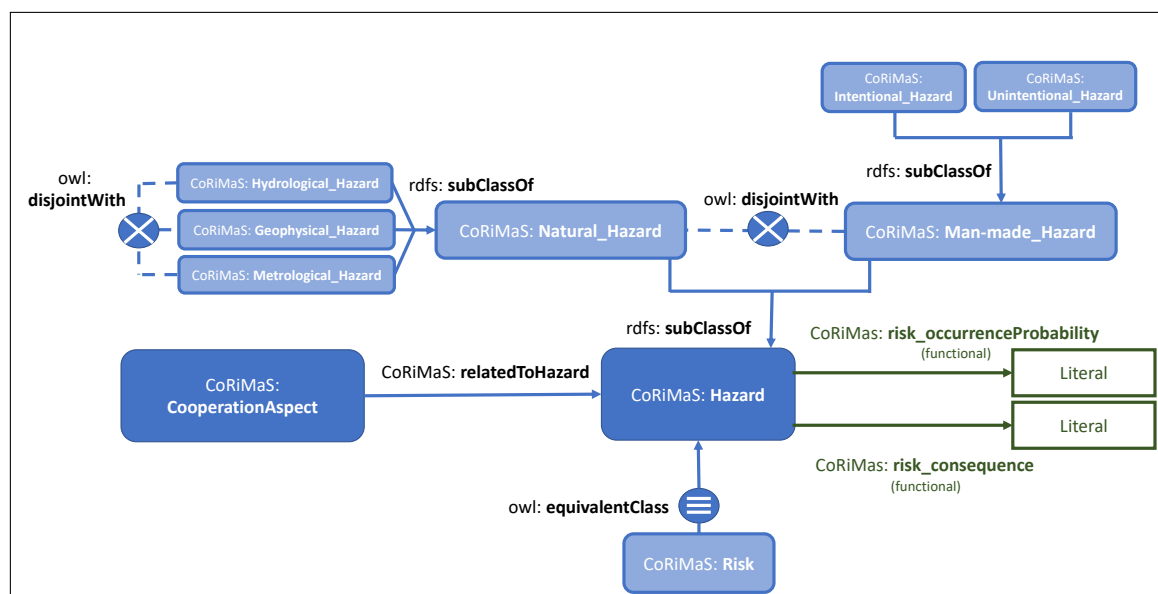


Figure 4. Hazard specification in CoRiMaS.

4.2. Stakeholder

A stakeholder can be defined within the ontology as a member of one of the equivalent classes *CoRiMaS:Stakeholder*, *CoRiMaS:Actor*, and *CoRiMaS:Player* (Figure 5). For stakeholders, the ontology provides a taxonomy for a proper classification from a risk management point of view. The model explicitly distinguished between internal and external stakeholders, represented by the corresponding ontological concepts *CoRiMaS:InternalStakeholder* and *CoRiMaS:ExternalStakeholder*. Apart from their involvement in the seaport, the most relevant semantic relationship involving stakeholders is the one to cooperation aspects (*CoRiMaS:relatedToStakeholder*). Typical attributes associated with institutions and individuals may be specified by using external vocabularies (e.g., vCard Ontology [57]).

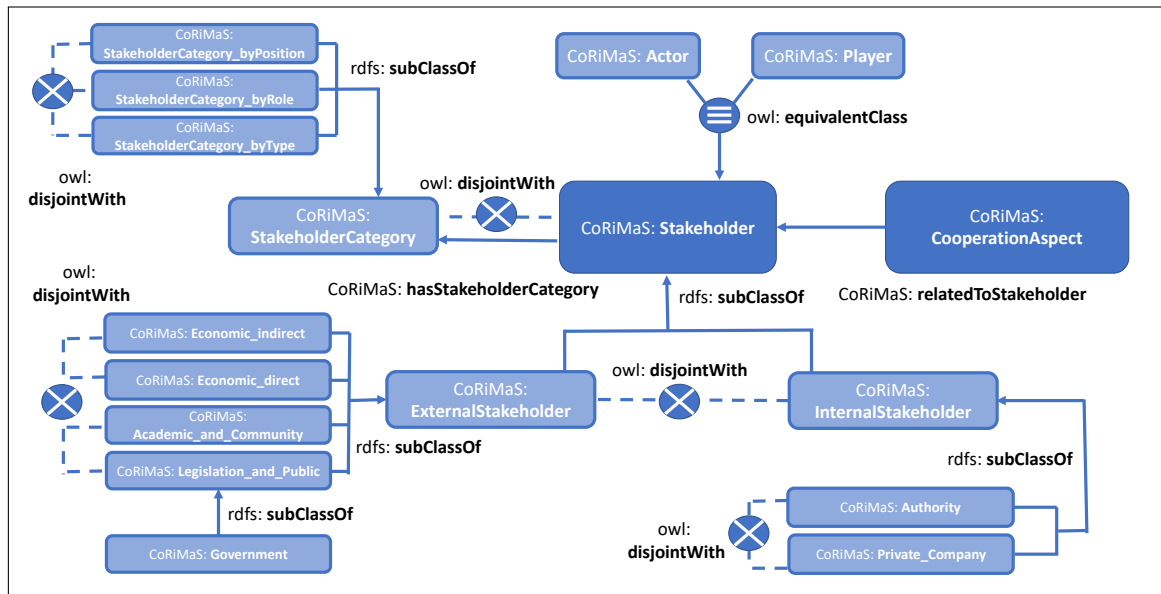


Figure 5. Stakeholder definition in CoRiMaS.

4.3. Seaport

As previously mentioned, a seaport is understood as a virtual organization (Figure 6) composed of a number of internal stakeholders that play an active role. Such a composition is stated by adopting the property *CoRiMaS:composedOf*. External stakeholders, which have some interest or are indirectly related to the port activities, may be associated with a given seaport by using one of the two equivalent properties *CoRiMaS:hasInterest* and *CoRiMaS:contributes*. As shown in Figure 6, a seaport may be characterised from a risk management perspective according to the CoRiMaS model with the support of a number of data and object properties. Although a detailed description of the specification is out of the scope of the paper, an example will be provided later on in the paper.

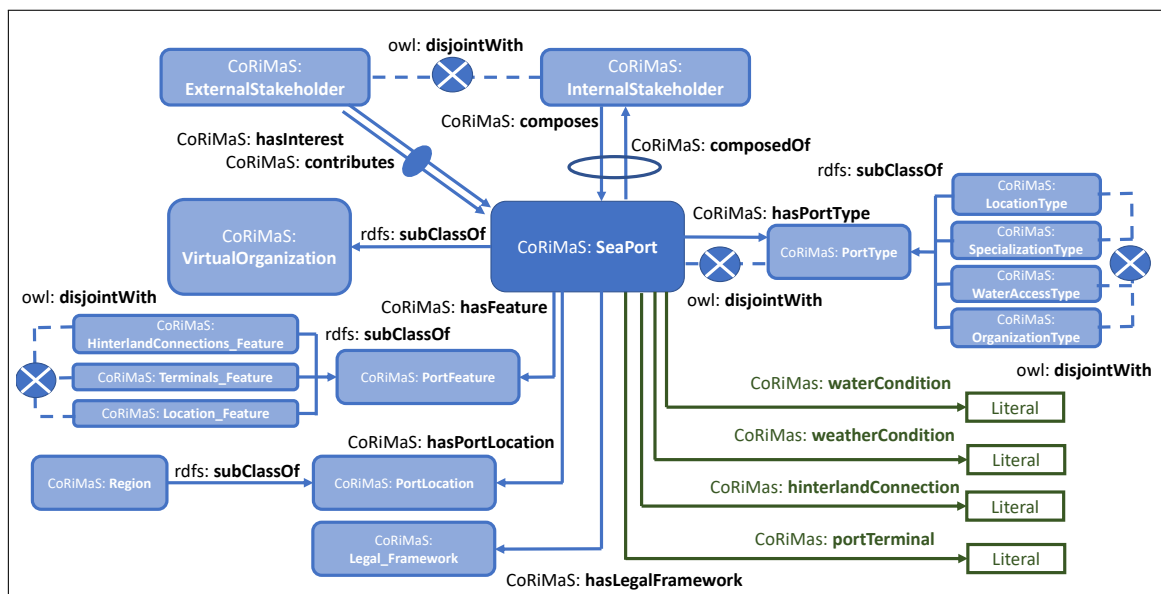


Figure 6. Seaport description in CoRiMaS.

4.4. Cooperation Aspect

As previously discussed in the paper, the cooperation aspect is the central concept in the CoRiMaS model and it is explicitly represented within the ontology by the *CoRiMaS:CooperationAspect*.

The ontological description of a cooperation aspect (Figure 7) reflects its original semantics and, indeed, it is related to target hazards (*CoRiMaS:relatedToHazard*), to the process established to manage such hazards (*CoRiMaS:relatedToProcess*) and to the stakeholder involved (*CoRiMaS:relatedToStakeholder*). Generic associations of internal/external concepts with a cooperation aspect may be established through the inverse pair of functions (see OWL specifications [44]) *CoRiMaS:aspectRelatedTo* and *CoRiMaS:relatedCooperationAspect*. Finally, further characterizations may be established by using the internal vocabulary or external ones.

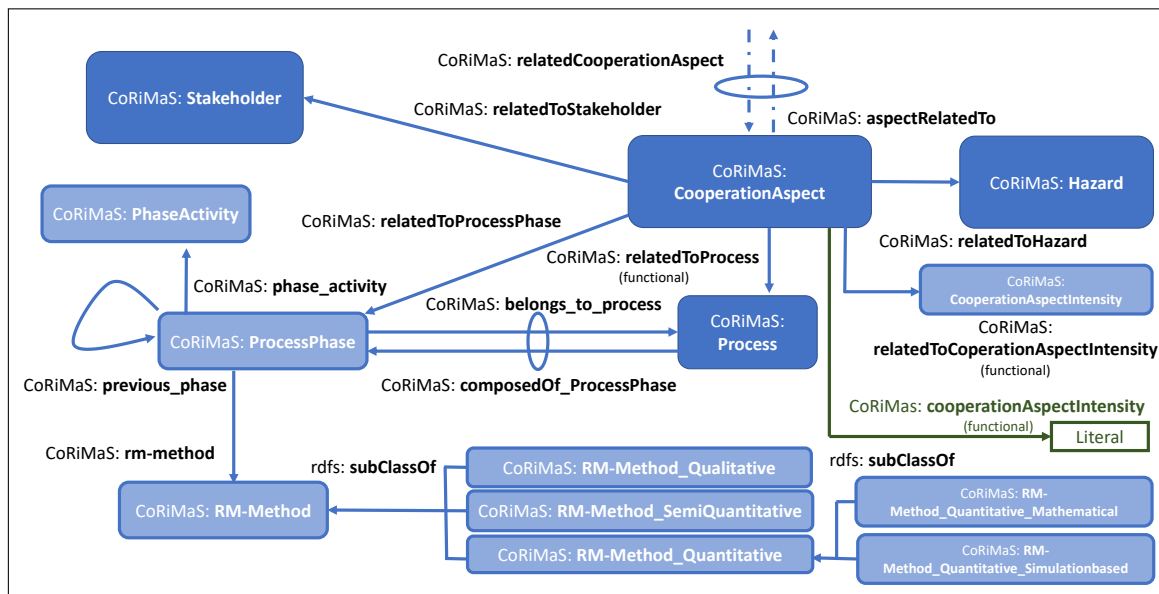


Figure 7. Specification of a cooperation aspect and related process in CoRiMaS.

4.5. Process

The use of ontology to describe general processes (e.g., [58]) or workflows (e.g., [59]) is quite common and extensively reported in literature. For instance, ontology-based semantic annotations may aim at establishing semantic interoperability among the different models [12], as well as at a re-use of components [60]. Likewise, ontology may describe domain-specific processes such as, among others, software processes [61], business processes [62], assembly processes [63], and relational processes [64].

We adopted an ad-hoc approach to provide a domain-specific concise description of risk management processes. These processes (*CoRiMaS:Process*) are understood as a sequence of phases (*CoRiMaS:ProcessPhase*). Each phase is associated with one or more risk management methods (*CoRiMaS:RM-Method*) and multiple activities (*CoRiMaS:PhaseActivity*) as defined in Tables 1 and 2. The ontology includes a taxonomy for risk management methods that distinguishes between qualitative, quantitative, and semi-quantitative methods.

5. A Case Study: The Port of Hamburg

As a case study, we refer to the Port of Hamburg (<https://www.hafen-hamburg.de/en/>). We first describe the current approach, focusing on generic risk management practices and limitations. Then, we provide some examples of practical use of the ontology within that context emphasizing on the added value provided.

5.1. Current Risk Management Systems and Practices at Port of Hamburg

One of the most important difficulties that stakeholders have when dealing with risk management at seaports is the lack of a standard process. Such a standard approach should be customized to tackle

different risk sources. For instance, at the Port of Hamburg, every stakeholder follows a different approach to deal with natural and man-made hazards.

Furthermore, due to this stakeholder-specific focus, roles and responsibilities for risk management are neither documented nor accessible for other stakeholders, especially for small and medium size companies. Assuming this kind of setup, cooperation is quite difficult as, at least in general, there is no central management and coordination of the different activities. Only some core stakeholders including authorities, shipping companies, and terminal operators implement some cooperation based on leadership, coordination, and consultations. However, the cooperation aspects carried out by these stakeholders are not always clearly defined and linked to specific processes and hazards.

As explained in the introductory part, the ontology object of this paper aims at establishing a common dynamic language to define a cooperative approach to risk management in seaports. Such a support is expected to facilitate analysis at any stage and to provide semantic linkage among responsible stakeholders, examined hazards, cooperation aspects, and the corresponding risk management processes. As shown in the next subsection, the complex scenario may be easily described through a formal specification supported by an extensible taxonomy and a set of relationships among concepts.

5.2. Application of the Ontology to the Port of Hamburg

In the next subsections we describe some aspects of the Port of Hamburg, addressing a number of real assets and components related to risk management.

An exhaustive description of such an environment would be quite long and articulated. That is definitely out of the scope of this paper.

Rather, we focus on the description of a number of selected aspects by adopting the data model provided. The subset considered shows the intrinsic complexity of the target scenario and, in our opinion, constitutes a validation for the CoRiMaS model and for its ontological implementation.

5.2.1. Describing Seaports

The Port of Hamburg is the third largest port in Europe and is located in the City State of Hamburg (Germany). The port is operated in a landlord model as premises are owned to the largest extent by the responsible Port Authority (<https://www.hamburg-port-authority.de/en/>) and are leased out to private companies based on long term contracts.

It is a tidal port that is effected by frequent water level changes with large ships entering or exiting during high tide. As a universal port, it can handle many different types of cargo. For processing the cargo, the port possesses terminals for containers, bulk, break bulk, and liquids. In addition, the port also handles an increasing amount of passengers at its cruise terminals. The cargo loads are further transported to hinterland destinations using rail, road, or inland waterway connections. The Port of Hamburg may be defined as a kind of virtual organization composed of a number of internal stakeholders that play an important role in its daily operational processes, such as the Hamburger Hafen und Logistik AG [65] (terminal operator), the Hapag-Lloyd AG (www.hapag-lloyd.com/en/home.html, shipping company) and the Hamburg Port Authority (<https://www.hamburg-port-authority.de/en/>). External stakeholders, such as the Berufsgenossenschaft für Handel und Warenlogistik (<https://www.bghw.de/>, employee liability insurance) and the Deutsche Bahn AG (<https://www.deutschebahn.com/en>, train company), contribute to the overall operations at the seaport, and have a keen interest in the activities carried out by the internal stakeholders. The stakeholders at the port of Hamburg follow various regional, national, and supranational regulations constituting the legal framework. Examples in this context are the International Ship and Port Facility Security Code (ISPS) and the Directive of the European Parliament and of the Council on Enhancing Port Security (Directive 2005/65/EC).

A formal description of the Port of Hamburg according to the CoRiMaS ontology is reported in Figure 8. As shown, the vocabulary provided, including concepts and relationships among them,

allows for a systematic unambiguous description of a complex reality. Such an explicit description is integrated by the inference capabilities inherent in the ontology. For instance, the stakeholders listed are automatically classified as internal or external stakeholders depending on the relationships (*CoRiMaS:composedOf* or *CoRiMaS:contributes* in the formal specification) existing between them and the seaport.

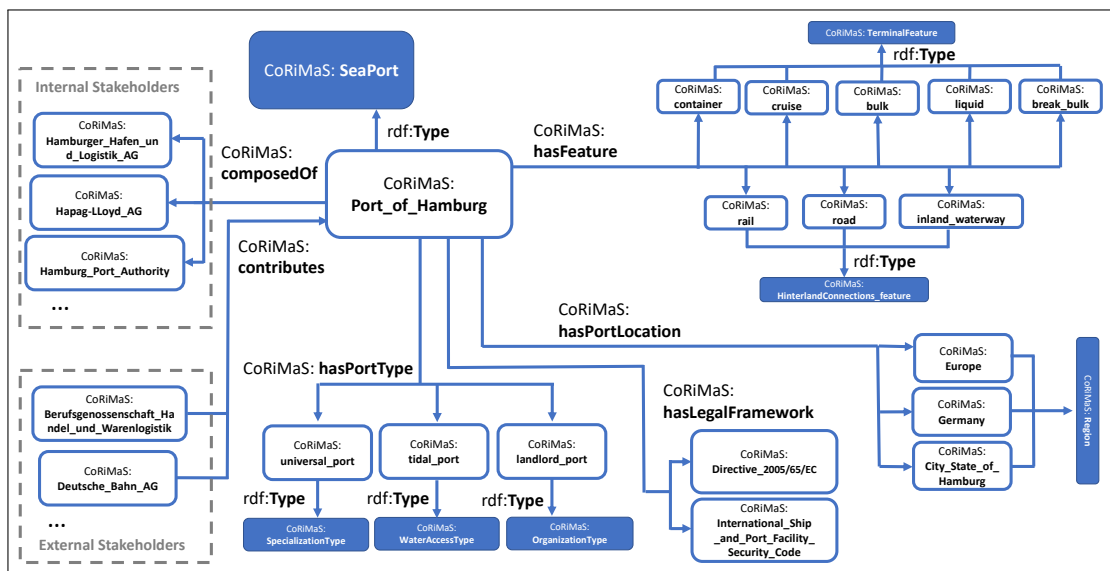


Figure 8. Formal description of the Port of Hamburg according to the CoRiMaS ontology.

5.2.2. Describing Stakeholders

Examples of stakeholders are reported in Figure 9.

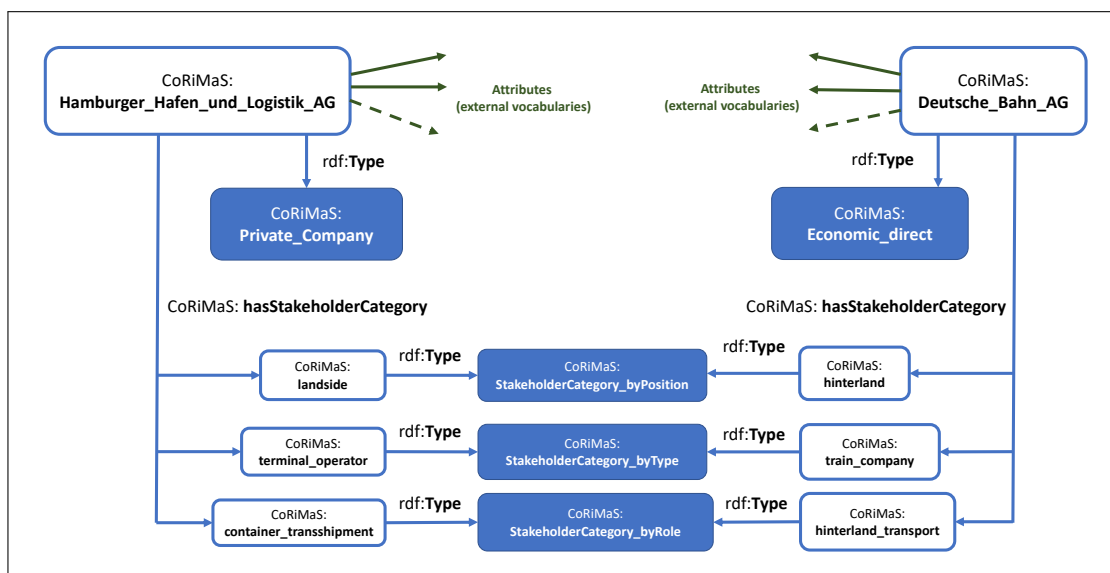


Figure 9. Example of stakeholder description.

The Hamburger Hafen und Logistik AG (HHLA) [65] is an internal stakeholder who engages in the daily activities at the seaport. It is a privately owned terminal operator that is located at the land side of the seaport. The company focuses, with its container hubs, on the transshipment of containers, connecting the seaport with the hinterland economic regions.

The Deutsche Bahn AG (DB) (<https://www.deutschebahn.com/en>) is an external stakeholder that is directly linked to the daily economic activities at the seaport. It is a train company, owning and

operating the largest part of the hinterland railway network. The DB network is connected to the port by the land side railway connection of the Hafengebahn (eng. Port Railway) which is operated by the Hamburg Port Authority.

Both stakeholders are described by adopting the standard categorization offered by the ontology. Indeed, HHLA is declared to be a private company (*CoRiMaS:Private_Company*) and DB to be an entity with a direct economic interest in the seaport (*CoRiMaS:Economic_direct*).

Furthermore, as shown in the diagram, a number of types are dynamically defined by adopting the rich vocabulary provided and are associated with the stakeholders. For instance, from a position perspective, the two stakeholders are associated with the types *CoRiMaS:landside* and *CoRiMaS:hinterland* respectively.

5.2.3. Describing Hazards

In the Port of Hamburg, several different hazards have to be considered during daily operations.

For instance, very frequently, incorrect or undeclared dangerous goods from all over the world represent a critical hazard in the process of cargo handling. As dispatchers and shippers are required to declare the transported goods truthfully, a violation of this practice is always a conscious act. Consequently, undeclared dangerous goods can be classified as intentional hazard. The resulting risk might heavily affect the port community as demonstrated by the case of the “CCNI AURACO” that is described in the introductory section.

An example of a hazard that might be either intentional or unintentional is the occurrence of an oil leakage. In most cases, an oil barrel or hydraulic line is not damaged by intention by the responsible person, although in few others it might have been a wilful act.

Apart from man-made hazards, natural hazards are also a critical source of risk. Storm surge is a hydrological hazard frequently witnessed in many regions, and in the Port of Hamburg in particular. Lightning, as an example of metro-logical hazards, is also relevant in most regions and represents therefore a hazard that needs to be considered.

Regardless of the hazard type, the resulting risk occurrence probability and risk consequence can be classified into different levels, either by qualitative or quantitative measures. In Hamburg, different assessment levels are used by the respective internal stakeholders and a commonly accepted classification does not exist. Here, as an example, we followed the universally applicable levels of low, medium, and high to assess identified risks. Terminal operators, for instance, follow different approaches to determine the risk occurrence probability and consequence. For example, dangerous goods are analysed and evaluated in a risk matrix or other hazard analysis method based on a designated class for dangerous goods (e.g., class 1: fireworks). A semi-quantitative scale (low-high) for the occurrence probability and consequence is used, and corresponding values are selected based on expert knowledge and previous incidents.

Our formal representations are proposed in Figure 10. The examples previously cited are associated with their respective categories as well as the associated risk occurrence probability and risk consequence is set as a variable range “low-high”.

5.2.4. Describing Cooperation Aspects

As an example of cooperation aspect, we propose joint exercises on leaking containers, which is considered one of the most critical cooperation aspects in the Port of Hamburg. It refers to dangerous goods as man-made hazards, because leakages from such containers represent a severe risk to health and the environment. As executing entities, internal stakeholders, such as terminal operators and fire brigades, are involved. In the case of Hamburg, the Hamburg Hafen und Logistik AG [65] receives support and training from the fire brigade in such exercises to increase their degree of preparedness and response capabilities. For instance, emergency plans are discussed and simulated in such exercises to mitigate the consequences of hazardous materials’ leakage from containers. The number of these joint exercises per year defines the cooperation intensity between the HHLA and the fire brigade. Each joint

exercise is carefully planned considering different resources and specific scenarios. The joint exercises on leaking containers are linked to the treatment phase of the dangerous goods management process.

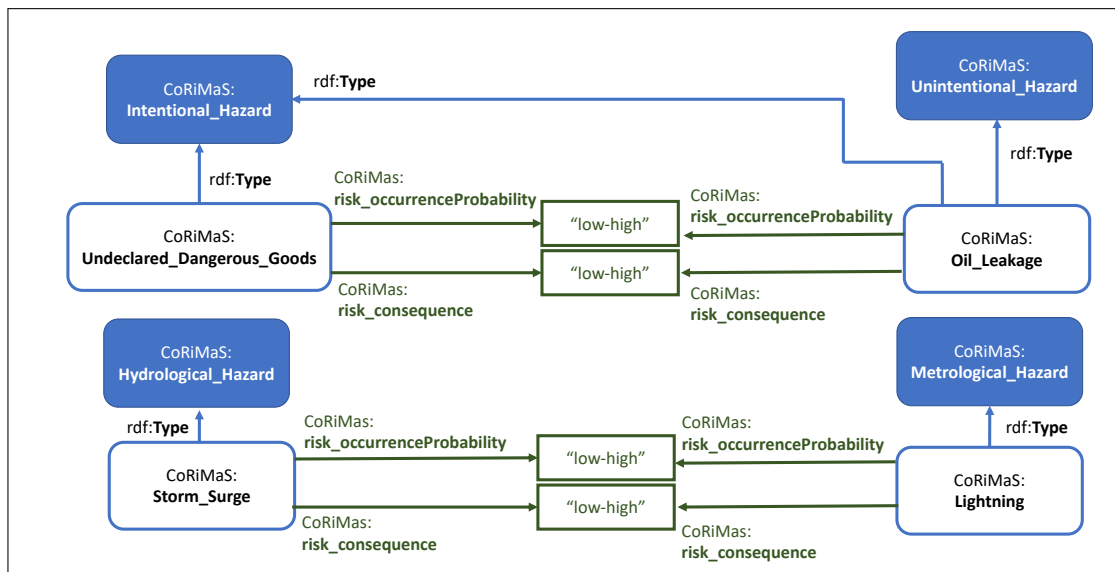


Figure 10. Example of hazard description.

The ontological representation for the target cooperation aspect is proposed in Figure 11. As shown, the cooperation aspect (CoRiMaS: Joint_Excercise_on_Leaking_Containers) is related to the target hazard (CoRiMaS: Dangerous_Goods), to the stakeholders involved (CoRiMaS: Hamburg_Hafen_und_Logistik_AG and CoRiMaS: Fire_Brigade in this case), and to process to follow (CoRiMaS: Dangerous_Goods_Management_Process).

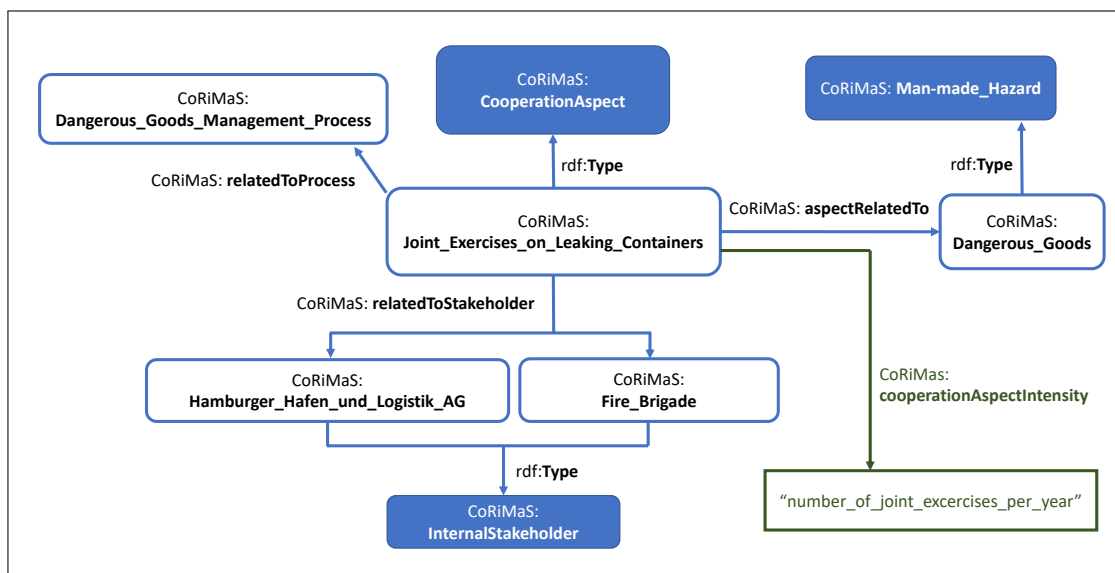


Figure 11. Specification of cooperation aspects.

5.2.5. Describing Processes

A generic management process for dangerous goods normally comprises four main phases: identification, analysis, evaluation, and treatment. Each phase consists of several activities that need to be carried out to deliver the intended result to the corresponding phase. Each phase uses specific methods that allows the successful implementation of the phase activities.

For risk identification, checklists are used to identify hazards and derive the associated potential risks. For instance, a standard checklist from the German Chemical Industry Association (Verband der Chemischen Industrie e. V., VCI) is used by the HHLA to identify dangerous goods in a container. In the risk analysis phase, the causes and consequences for a leaking container are identified along with assessing the risk occurrence probability and consequence. These activities are fulfilled using the Preliminary Hazard Analysis (PHA) method (System Safety Program Requirements, MIL-STD-882c, 1993). PHA is a risk analysis method used to identify potential hazards. It should consider environmental constraints, hazardous components, and safety-related equipment. The evaluation phase follows in order to define the evaluation criteria and treatment priorities. The hazard diamond, also called fire diamond, is presented in the NFPA (704) which is the Standard System for the Identification of the Hazards of Materials for Emergency Response (Standard System for the Identification of the Hazards of Materials for Emergency Response, NFPA 704, 2017). The four divisions of the diamond, health hazard, chemical reactivity, flammability, and special hazards are used by fire brigades to evaluate hazardous materials as well as to derive the treatment precautions and priorities. Based on the evaluation phase, the identification and deployment of suitable counter measures are required in the treatment phase. Additionally, the definition of responsibilities for the deployment of measures among fire brigades and the HHLA is carried out. A catalogue for hazardous materials and dangerous goods is used as a method to derive the suitable counter measures based on the evaluation phase carried out using the HAZARD diamond.

The whole process is formally described by the diagram in Figure 12 as a composition of the different phases, each of whom is associated with activities and related methods.

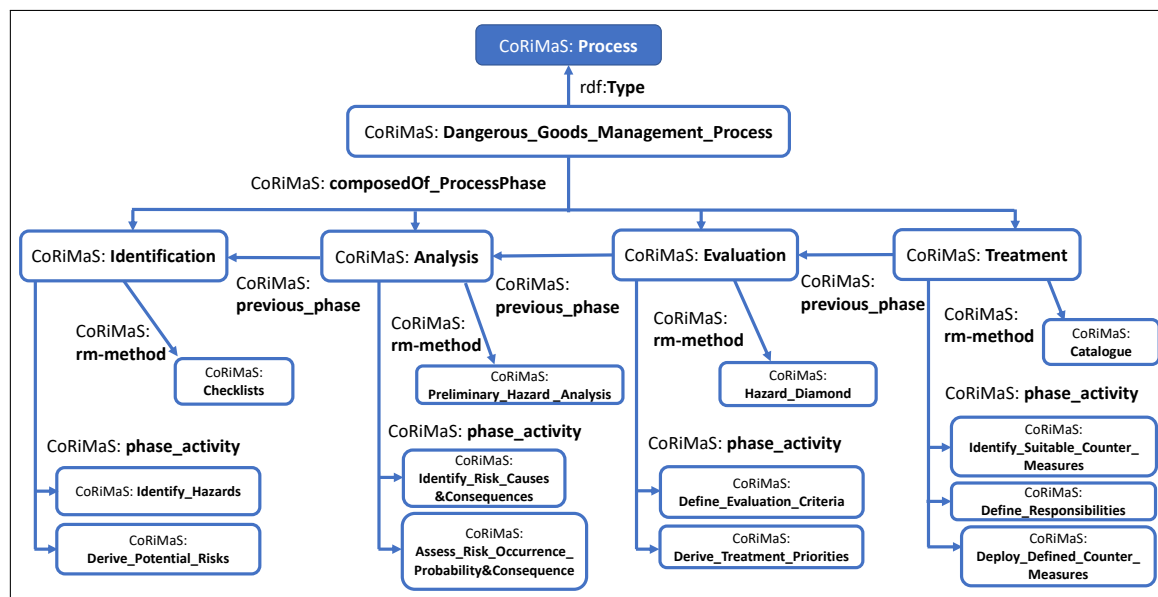


Figure 12. An example of risk management process specification.

6. Applications

As extensively discussed in the paper, CoRiMaS underpins the formal representation of existing seaports and hazard-related issues. This representation defines a kind of mapping as the function of types, features, locations, legal frameworks, as well as internal and external stakeholders. Such a mapping enables in practice a large amount of information within a unique knowledge framework defined according to a rich data model.

Within that same knowledge framework, risk management processes and cooperation aspects may be easily defined and formally specified. According to this descriptive approach, specific methods, countermeasures, tasks, and responsibilities of corresponding internal stakeholders are linked to the structure of a seaport, corresponding stakeholders, recommended processes, and hazards.

This enhanced capability in terms of analysis is expected to contribute in the future development of a more prescriptive model for cooperative risk management in seaports.

More concretely, we consider the application of the ontology at three different levels:

- *Data/Knowledge Infrastructure.* We believe our ontology may be primarily understood as a contribution to the development of the Semantic Web.
- *Applications within Knowledge-based Systems.* We also aim at the application within generic knowledge-based systems, in which the ontology may contribute to an effective knowledge management approach [66] in a context wider than the specific risk management. For instance, internal documents on risk management may be enriched with semantic annotations and can be linked to other information sources internally as well as externally.
- *Expert Systems.* The intent and the extent of our ontology is much beyond an unique specific expert system. Indeed, we designed this knowledge infrastructure having in mind a cutting edge scenario in which a centralized system is composed by multiple expert systems that are interconnected by interchanging information and data. We are confident that this philosophy can meet most practical requirements in the context of a complex virtual organization. It implicitly enables the interchange of data also across heterogeneous systems and, of course, among different seaports to provide a further level of analysis and consolidation for processes, methods, and underlining strategies.

7. Conclusions and Future Work

This paper describes an ontological approach for cooperative risk management in seaports. The model proposed and its formal specification enable the effective description and re-use of risk management activities and their related environments, the analysis of current strategies for specific risks, and the continuous alignment and optimization. Indeed, the complex structure of seaports requires the definition of clear standards, regulations, processes, roles, and responsibilities.

A case study conducted for the Port of Hamburg was used to validate the developed ontology. The experiment shows the strong connection among the concept classes defined within the ontology and the applicability of the defined relationships among the different concepts, as well as the flexibility of the proposed vocabulary, which relies on extensible and customizable constructs.

The CoRiMaS ontology was developed to be widely applicable and to foster cooperation within and among seaports. We believe that, if properly used, it may significantly contribute to improve risk management and, thereby, to increase the resilience of operations within seaports, as well as the protection of surrounding areas. By focusing on a collaborative approach, we are intrinsically assuming that common potential conflicts of interest, normally raising within virtual organizations and related to economic implications, exist, but are not as relevant as the common goal to improve safety in operations.

Additionally, we consider the descriptive characteristics of the ontological approach to be potentially helpful in the development of a more prescriptive model for cooperative risk management in seaports. This will definitely help single stakeholders, as well helping to further encourage the cooperation among them to improve the management of risks during each phase of the risk management process.

Current limitations are mainly related to the very limited experimentation; however, our main contribution is the formal specification of the model. We believe that this formalization of the framework may facilitate its adoption in practice. A further and deeper validation in the context of the Port of Hamburg and other seaports will be the object of future work. Such a consolidation phase is expected to drive the evolution of the core ontology as presented in this paper. As extensively discussed, the ontology is developed upon semantic technology and, therefore, can provide a solid support to develop sophisticated knowledge-based systems and, in general, for applications that require data aggregation, re-use, and interoperability.

Author Contributions: Conceptualization, all authors; formal analysis, S.F.P., M.I., and A.N.; investigation, all authors; methodology, S.F.P., M.I., and A.N.; validation, M.I. and A.N.; visualization: S.F.P.; writing—original draft preparation, all authors; writing—review and editing, all authors. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the European Regional Development Fund (ERDF) and the European Neighbourhood Instrument (ENI) within the scope of the Interreg Baltic Sea Region Programme through the EUSBSR flagship project HAZARD (<http://blogit.utu.fi/hazard/>). Publishing fees supported by Funding Programme “Open Access Publishing” of Hamburg University of Technology (TUHH).

Acknowledgments: We would like to thank Iwona Miliszewska for supporting the collaboration between UTS and TUHH. Additionally, we would like to thank the anonymous reviewers for the constructive feedback provided.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. UNCTAD—Review of Maritime Transport 2019. Available online: https://unctad.org/en/PublicationsLibrary/rmt2019_en.pdf (accessed on 27 May 2020).
2. Destatis—Gefahrguttransporte 2017. Available online: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Transport-Verkehr/Publikationen/Downloads-Querschnitt/gefahrguttransporte-2080140177004.pdf?__blob=publicationFile (accessed on 27 May 2020).
3. Major Fire on Container Ship CCNI Arauco in Hamburg—Maritime Harold [Online]. Available online: <http://www.maritimeherald.com/2016/major-fire-on-container-ship-ccni-arauco-in-hamburg/> (accessed on 8 January 2018).
4. Annual Overview of Marine Casualties and Incidents 2018. Available online: <http://www.emsa.europa.eu/news-a-press-centre/external-news/item/3406-annual-overview-of-marine-casualties-and-incidents-2018.html> (accessed on 29 April 2019).
5. Nagi, A.; Indorf, M.; Kersten, W. Bibliometric analysis of risk management in seaports. In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL)*; epubli GmbH: Berlin, Germany, 2017; Volume 23, pp. 491–521.
6. Guarino, N. Formal ontology, conceptual analysis and knowledge representation. *Int. J. Hum. Comput. Stud.* **1995**, *43*, 625–640. [[CrossRef](#)]
7. Pileggi, S.F.; Lopez, A.; Beydoun, G. Ontology in Software Engineering. In Proceedings of the 29th Australasian Conference on Information Systems, Sydney, Australia, 3–5 December 2018.
8. Guarino, N.; Oberle, D.; Staab, S. What is an ontology? In *Handbook on Ontologies*; Springer: Berlin, Germany, 2009; pp. 1–17.
9. Gardner, S.P. Ontologies and semantic data integration. *Drug Discov. Today* **2005**, *10*, 1001–1007. [[CrossRef](#)]
10. Berners-Lee, T.; Hendler, J.; Lassila, O. The semantic web. *Sci. Am.* **2001**, *284*, 34–43. [[CrossRef](#)]
11. Bizer, C. The emerging web of linked data. *IEEE Intell. Syst.* **2009**, *24*, 87–92. [[CrossRef](#)]
12. Lin, Y.; Ding, H. Ontology-based semantic annotation for semantic interoperability of process models. In Proceedings of the International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC’06), Vienna, Austria, 28–30 November 2005.
13. Alyami, H.; Yang, Z.; Riahi, R.; Bonsall, S.; Wang, J. Advanced uncertainty modelling for container port risk analysis. *Accid. Anal. Prev.* **2019**, *123*, 411–421. [[CrossRef](#)] [[PubMed](#)]
14. Ding, J.F.; Tseng, W.J. Fuzzy risk assessment on safety operations for exclusive container terminals at Kaohsiung port in Taiwan. *Proc. Inst. Mech. Eng. Part M J. Eng. Marit. Environ.* **2013**, *227*, 208–220. [[CrossRef](#)]
15. Mokhtari, K.; Ren, J.; Roberts, C.; Wang, J. Decision support framework for risk management on sea ports and terminals using fuzzy set theory and evidential reasoning approach. *Expert Syst. Appl.* **2012**, *39*, 5087–5103. [[CrossRef](#)]
16. Mokhtari, K.; Ren, J.; Roberts, C.; Wang, J. Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. *J. Hazard. Mater.* **2011**, *192*, 465–475. [[CrossRef](#)]

17. Wan, C.; Yan, X.; Zhang, D.; Yang, Z. Analysis of risk factors influencing the safety of maritime container supply chains. *Int. J. Shipp. Transp. Logist.* **2019**, *11*, 476–507. [[CrossRef](#)]
18. Trbojevic, V.M.; Carr, B.J. Risk based methodology for safety improvements in ports. *J. Hazard. Mater.* **2000**, *71*, 467–480. [[CrossRef](#)]
19. Belamarić, G.; Kurtela, Ž.; Bošnjak, R. Simulation method-based oil spill pollution risk analysis for the port of šibenik. *Trans. Marit. Sci.* **2016**, *5*, 141–154. [[CrossRef](#)]
20. Roh, S.; Tam, J.; Lee, S.W.; Seo, Y.J. Risk assessment of maritime supply chain security in ports and waterways. *Int. J. Supply Chain Manag.* **2018**, *7*, 300–307.
21. Izaguirre, C.; Losada, I.J.; Camus, P.; González-Lamuño, P.; Stenek, V. Seaport climate change impact assessment using a multi-level methodology. *Marit. Policy Manag.* **2020**, 1–14. [[CrossRef](#)]
22. Sciarriello, R.; Zuzolo, D.; Cicchella, D.; Iannone, F.; Cammino, G.; Guarino, C. Contamination and ecological risk assessment of the seaport of Naples (Italy): Insights from marine sediments. *J. Geochem. Explor.* **2020**, *210*, 106449. [[CrossRef](#)]
23. Kron, W. Coasts: The high-risk areas of the world. *Nat. Hazards* **2013**, *66*, 1363–1382. [[CrossRef](#)]
24. Cao, X.; Lam, J.S.L. Simulation-based severe weather-induced container terminal economic loss estimation. *Marit. Policy Manag.* **2019**, *46*, 92–116. [[CrossRef](#)]
25. Gong, Z.; Liu, N. Mitigative and adaptive investments for natural disasters and labor strikes in a seaport–dry port inland logistics network. *Marit. Policy Manag.* **2020**, *47*, 92–108. [[CrossRef](#)]
26. Loh, H.S.; Thai, V.V. Management of disruptions by seaports: preliminary findings. *Asia Pac. J. Mark. Logist.* **2015**, *27*, 146–162. [[CrossRef](#)]
27. Pachakis, D.; Kiremidjian, A.S. The use of simulation in disaster response planning and risk management of ports and harbors. In *Advancing Mitigation Technologies and Disaster Response for Lifeline Systems*; Amer Society of Civil Engineers: Reston, VA, USA, 2003; pp. 425–434.
28. Cho, H.S.; Lee, J.S.; Moon, H.C. Maritime Risk in Seaport Operation: A Cross-Country Empirical Analysis with Theoretical Foundations. *Asian J. Shipp. Logist.* **2018**, *34*, 240–248. [[CrossRef](#)]
29. Kadir, Z.A.; Mohammad, R.; Othman, N.; Amrin, A.; Muhtazaruddin, M.N.; Abu-Bakar, S.H.; Muhammad-Sukki, F. Risk Management Framework for Handling and Storage of Cargo at Major Ports in Malaysia towards Port Sustainability. *Sustainability* **2020**, *12*, 516. [[CrossRef](#)]
30. Ekelhart, A.; Fenz, S.; Klemen, M.; Weippl, E. Security ontologies: Improving quantitative risk analysis. In Proceedings of the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA, 3–6 January 2007.
31. Birkholz, H.; Sieverdingbeck, I.; Sohr, K.; Bormann, C. IO: An interconnected asset ontology in support of risk management processes. In Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security (ARES), Prague, Czech Republic, 20–24 August 2012; pp. 534–541.
32. Tserng, H.P.; Yin, S.Y.; Dzung, R.; Wou, B.; Tsai, M.; Chen, W. A study of ontology-based risk management framework of construction projects through project life cycle. *Autom. Constr.* **2009**, *18*, 994–1008. [[CrossRef](#)]
33. Ekelhart, A.; Fenz, S.; Neubauer, T. Ontology-based decision support for information security risk management. In Proceedings of the 2009 Fourth International Conference on Systems, Guadeloupe, France, 1–6 March 2009; pp. 80–85.
34. Wang, H.H.; Boukamp, F. Ontology-based representation and reasoning framework for supporting job hazard analysis. *J. Comput. Civ. Eng.* **2011**, *25*, 442–456. [[CrossRef](#)]
35. Wu, C.G.; Xu, X.; Zhang, B.K.; Na, Y.L. Domain ontology for scenario-based hazard evaluation. *Saf. Sci.* **2013**, *60*, 21–34. [[CrossRef](#)]
36. Blanc Alquier, A.; Lagasse Tignol, M. Risk management in small-and medium-sized enterprises. *Prod. Plan. Control* **2006**, *17*, 273–282. [[CrossRef](#)]
37. Liu, G.; Wang, Y.; Wu, C. Research and application of geological hazard domain ontology. In Proceedings of the 2010 18th International Conference on Geoinformatics, Beijing, China, 18–20 June 2010; pp. 1–6.
38. Lorens, P. Urban Waterfront Regeneration: Origins of the Issue. 2014. Available online: <https://mostwiedzy.pl/pl/publication/urban-waterfront-regeneration-origins-of-the-issue,130478-1> (accessed on 25 January 2019).
39. Center for Chemical Process Safety. *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd ed.; Wiley-Interscience: Hoboken, NJ, USA, 1999; ISBN 9780816907205. [[CrossRef](#)]

40. Kaundinya, I.; Nisancioglu, S.; Kammerer, H.; Oliva, R. All-hazard guide for transport infrastructure. *Transp. Res. Procedia* **2016**, *14*, 1325–1334. [[CrossRef](#)]
41. Maloni, M.J.; Jackson, E.C. Stakeholder Contributions to Container Port Capacity: A Survey of Port Authorities. *J. Transp. Res. Forum* **2010**, *46*. [[CrossRef](#)]
42. Gharehgozli, A.H.; Mileski, J.; Adams, A.; von Zharen, W. Evaluating a “wicked problem”: A conceptual framework on seaport resiliency in the event of weather disruptions. *Technol. Forecast. Soc. Chang.* **2017**, *121*, 65–75. [[CrossRef](#)]
43. *Standards Australia/Standards New Zealand, Risk Management: Australian/New Zealand Standard: AS/NZS 4360:2004*, 3rd ed.; Standards Australia: Sydney, Australia, 2004.
44. OWL 2 Web Ontology Language, Document Overview (Second Edition). Available online: <https://www.w3.org/TR/owl2-overview/> (accessed on 12 December 2018).
45. Gennari, J.H.; Musen, M.A.; Ferguson, R.W.; Grosso, W.E.; Crubézy, M.; Eriksson, H.; Noy, N.F.; Tu, S.W. The evolution of Protégé: an environment for knowledge-based systems development. *Int. J. Hum. Comput. Stud.* **2003**, *58*, 89–123. [[CrossRef](#)]
46. Glimm, B.; Horrocks, I.; Motik, B.; Stoilos, G.; Wang, Z. HermiT: an OWL 2 reasoner. *J. Autom. Reason.* **2014**, *53*, 245–269. [[CrossRef](#)]
47. WebVOWL: Web-Based Visualization of Ontologies. Available online: <http://vowl.visualdataweb.org/webvowl.html> (accessed on 24 April 2019).
48. Lohmann, S.; Negru, S.; Haag, F.; Ertl, T. Visualizing Ontologies with VOWL. *Semant. Web* **2016**, *7*, 399–419. [[CrossRef](#)]
49. RDF Schema 1.1. Available online: <https://www.w3.org/TR/rdf-schema/> (accessed on 24 April 2019).
50. Sirin, E.; Parsia, B.; Grau, B.C.; Kalyanpur, A.; Katz, Y. Pellet: A practical owl-dl reasoner. *Web Semant. Sci., Serv. Agents World Wide Web* **2007**, *5*, 51–53. [[CrossRef](#)]
51. ARQ—A SPARQL Processor for Jena. Available online: <https://jena.apache.org/documentation/query/> (accessed on 24 April 2019).
52. Schmidt, J.; Matcham, I.; Reese, S.; King, A.; Bell, R.; Henderson, R.; Smart, G.; Cousins, J.; Smith, W.; Heron, D. Quantitative multi-risk analysis for natural hazards: a framework for multi-risk modelling. *Nat. Hazards* **2011**, *58*, 1169–1192. [[CrossRef](#)]
53. Bergqvist, R.; Monios, J. *Green Ports: Inland and Seaside Sustainable Transportation Strategies*; Elsevier: Amsterdam, The Netherlands, 2018.
54. Camarinha-Matos, L.M.; Afsarmanesh, H. *Tendencies and general requirements for virtual enterprises*; Springer: Boston, MA, USA, 1999; pp. 15–30.
55. Liu, C.; Cheng, F.; Han, Y. SATOR: A scalable resource registration mechanism enabling virtual organizations of enterprise applications. In *International Conference on Grid and Cooperative Computing*; Springer: Berlin, Germany, 2005; pp. 744–749.
56. Nassar, P.B.; Badr, Y.; Barbar, K.; Biennier, F. Risk management and security in service-based architectures. In *Proceedings of the 2009 International Conference on Advances in Computational Tools for Engineering Applications*, Zouk Mosbeh, Lebanon, 15–17 July 2009; pp. 214–218.
57. vCard Ontology—For describing People and Organizations. Available online: <https://www.w3.org/TR/vcard-rdf/> (accessed on 16 January 2018).
58. Aitken, S.; Curtis, J. A process ontology. In *International Conference on Knowledge Engineering and Knowledge Management*; Springer: Berlin, Germany, 2002; pp. 108–113.
59. Haller, A.; Oren, E.; Kotinurmi, P. m3po: An ontology to relate choreographies to workflow models. In *Proceedings of the 2006 IEEE International Conference on Services Computing (SCC'06)*, Chicago, IL, USA, 18–22 September 2006; pp. 19–27.
60. Lin, Y.; Strasunskas, D. Ontology-based semantic annotation of process templates for reuse. *Proc. CAiSE* **2005**, *5*, 593–604.
61. Liao, L.; Qu, Y.; Leung, H. A software process ontology and its application. In *Semantic Web Enabled Software Engineering*; IOS-Press: Amsterdam, The Netherlands, 2014; Volume 17, pp. 207–217. [[CrossRef](#)]
62. Hepp, M.; Roman, D. An ontology framework for semantic business process management. In *eOrganisation: Service-, Prozess-, Market-Engineering*; Universitätsverlag Karlsruhe: Karlsruhe, Germany, 2007.

63. Lohse, N.; Hirani, H.; Ratchev, S.; Turitto, M. An ontology for the definition and validation of assembly processes for evolvable assembly systems. In Proceedings of the 6th IEEE International Symposium on Assembly and Task Planning: From Nano to Macro Assembly and Manufacturing, Montreal, QC, Canada, 19–21 July 2005; pp. 242–247.
64. Stout, M.; Love, J.M. Relational process ontology: A grounding for global governance. *Adm. Soc.* **2015**, *47*, 447–481. [[CrossRef](#)]
65. Hamburger Hafen und Logistik AG (HHLA). Available online: <https://hhl.de/en/home.html> (accessed on 16 January 2018).
66. Maedche, A.; Motik, B.; Stojanovic, L.; Studer, R.; Volz, R. Ontologies for enterprise knowledge management. *IEEE Intell. Syst.* **2003**, *18*, 26–33. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).