Context-Driven Dynamic Risk Management for Maritime Domain Awareness

Rafael Falcon*†, Benjamin Desjardins†, Rami Abielmona*† and Emil Petriu†
* Research & Engineering Division, Larus Technologies Corporation, Ottawa, Canada
† School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada
Email: rafael.falcon@larus.com, bdesj038@uottawa.ca, rami.abielmona@larus.com, petriu@uottawa.ca

***Abstract*—Endowing Decision Support Systems (DSSs) with a risk-aware view of the environment they operate in is critical to maintaining an acceptable level of Situational Awareness (SAW) as well as helping decision makers arrive at more accurate and timely conclusions. In particular, determining the situational elements that are presently impacting the system behaviour – and to what extent– leads to a refined SAW picture and ensures valuable knowledge propagation to the upstream layers of the underlying fusion/decision making process.**

In this paper, we augment an existing Risk Management Framework (RMF) with a set of atomic risk models capturing different situational elements. Contextual information feeding the DSS is employed to either activate one or more of these models or tailor their internal risk assessment. We show how context-aware dynamic risk management can be achieved in a DSS governed by the proposed architecture. Two maritime scenarios (vessel encountering active weather and vessel navigating in a piracy-infested region) serve to illustrate the advantages of the proposed context-aware methodology in terms of improved situational understanding, system interpretability, support to other fusion processes (e.g., threat assessment) and computational tractability. To the best of our knowledge, this is the first time that contextual information is used to drive the risk assessment module of a DSS. The methodology is not exclusive to the maritime arena and can be easily extrapolated to other domains.

I. Introduction

Surveying a region of interest in the Big Data era that we all live in [1] brings about significant challenges in terms of data collection, cleansing, mining and visualization. The ingestion and processing of these massive datasets, characterized by their volume, velocity and variety, is no longer a task humans can undertake on their own. Instead, this responsibility is often transferred to a Decision Support System (DSS) in order to create and maintain a representative model of the region under consideration in real time. DSSs [2] [3] are capable of drawing relevant information from the tide of incoming data and presenting it to the human operator in a more succint and amenable fashion. Human experts then make operational decisions by considering the DSS-generated information in light of their own domain expertise.

Risk management is an integral component of the decision making process as it enables the operator to identify and evaluate risky units, situations and environments as well as define, assess and select the most suitable courses of action to mitigate the perceived risks in the system. Regrettably, most of the modern DSSs still lack the integration of an end-to-end perceptual view of the multiple risk sources affecting the deployed environment. This is supported by little or no mention of risk management in several DSS reviews [2] [4] [3] or commercially available DSS products.

A solution to integrate risk into the core of any DSS came about five years ago when the authors in [5] introduced a *Risk Management Framework* (RMF). This multimodular architecture is able to (i) extract a parallel risk stream from the original stream fed by both hard and soft data sources without requiring any complementary information; this is accomplished by defining a set of *risk features*; (ii) assess in real time the *local risk* of any system unit with respect to a particular risk feature and its *overall risk* across all risk features; (iii) *visualize* the system's risk landscape at any point in time via evolving clustering algorithms, which allows for a more refined definition of the information granules behind the set of risk features and a proactive identification of the risky system units and (iv) the automatic generation of a set of *potential responses* to mitigate the identified system risks. Since its inception, the RMF has been continuously augmented with more technical capabilities and use cases in different application domains [6] [7] [8] [9].

In this paper, we expand the aforementioned RMF by tackling two existing limitations: (i) the lack of a *contextual information*[1] engine and (ii) the ability to ascribe risk to well-defined *situational elements* that are presently blended into one monolithic risk evaluation. This means that, in its current form, the RMF cannot deduce which situational elements have a stronger impact on the overall risk of any system unit. Our contributions are as follows: (i) we endow the RMF with a *Dynamic Risk Assessment Module* (DRAM) that is fed by contextual information and hosts a set of user-defined *atomic risk models*; (ii) we show how the contextual information, drawn from the *Contextual Knowledge Base* (CKB), is able to activate one or more of these atomic risk models or tailor their internal risk assessment; (iii) we illustrate our proposed framework in presence of three atomic risk models, namely *piracy*, *open water* and *active weather*, and two maritime scenarios (an act of piracy and the capsizing of a sailing vessel); (iv) we highlight the advantages of the proposed context-aware methodology in terms of improved situational understanding,

[1]Contextual information is any known information about the environment or its entities, with static and/or dynamic features, that could be exploited to improve the surveillance experience.

system interpretability, support to other fusion processes (e.g., threat assessment) and computational tractability. To the best of our knowledge, this is the first time that context is used to drive the risk assessment module of a DSS. The methodology is not exclusive to the maritime environment and can be easily extrapolated to other domains.

The remainder of the paper is structured as follows. Section II briefly goes over several relevant works. The RMF augmentation with the context-driven dynamic risk management features is discussed in Section III. The three atomic risk models and their associated contextual information as applied to the maritime domain are described in Section IV. The two case studies (maritime scenarios) used to showcase the advantages of our proposal are outlined in Section V before conclusions and future work are enunciated in Section VI.

II. Related Work

This Section briefly discusses relevant published works on risk analysis and contextual awareness in the maritime domain.

A. Maritime Risk Analysis

An important dimension of risk management for the maritime domain is to provide the set of processes and tools that support and enhance the operator's *situational awareness picture* (SAP). Several tools have been proposed in the literature to develop a system-level risk picture. *Hidden Markov Models* [10][11] (HMMs) are recurrently used in this domain to approximate the dynamics of the system-level risk picture. While HMMs provide an effective method for modeling tactical risk, they can be unstable in a dynamic environment when evaluating system-wide risks. The interdependence from one model to another makes the system stability vulnerable when reacting to unforeseen environment changes. Sustaining the integrity of large systems composed of many interconnected HMMs entails a steep cost. The same issue arises when relying on other probabilistic models such as *Bayesian Networks* [12].

Falcon et. al. [6] perform a risk-based multi-criteria decision analysis on a vessel in distress (VID) to automatically generate a set of promising potential responses. The methodology revolves around the RMF being augmented in this paper. In [9], the authors convert the output of maritime anomaly detectors into risk features and integrate them into the RMF to detect potential VIDs.

An avenue for risk assessment methodologies in the military realm stems from *complex systems research*, which includes *computational red teaming* [13][14] and *adversarial modelling* [15]. Among the existing risk-aware DSSs we can mention Raytheon's ATHENA Integrated Defense System [16], US Coast Guard's *Maritime Automatic Super Track Enhanced Reporting* (MASTER) and Comprehensive Maritime Awareness (CMA) [17] vessel tracking systems and DARPA's *Predictive Analysis for Naval Deployment Activities* (PANDA) [18].

B. Contextual Awareness in the Maritime Domain

Razavi et. al. [19] employ Natural Language Processing (NLP) techniques to extract risk spans from contextual information in the form of maritime incident reports. The proposed textual risk mining system applies a variety of sequence classification algorithms to compare the risk classification performance. Contextual data pertaining to real-world maritime incident reports and synthetically generated response descriptions, respectively, is brought in [8] and [20] into their RMF to better characterize a vessel's risk-driven SAP (Level 2 Fusion) and the set of potential responses to mitigate the perceived risk (Level 3 Fusion).

Garcia et al. [21] designed a harbor surveillance system combining ontology-based context representation, deductive reasoning for anomaly detection and abductive reasoning under uncertainty. They mixed key-value, ontology-based and logic-based models and employed the Belief-based Argumentation System to decide between two hypotheses (inaccurate/unreliable observations vs. possible threatening behavior) when a vessel cannot be classified by the "normal" classes.

In [22] the authors pinpoint several ways of modeling contextual information within the fusion process and elaborated on three main research areas in context-dependent situations.

III. Context-Driven Dynamic Risk Management

This Section elaborates on the extension of the RMF described in [5] and [6] with the inclusion of context-driven dynamic risk models.

A *risk model* $\mathcal{RM}$ is represented in the RMF by a tuple $\langle DF, RF, \gamma, \rho, \rho^* \rangle$ where DF and RF are the set of (raw) data and risk features, respectively and $\gamma : DF^k \rightarrow RF$ is the mapping that transforms an arbitrary number k of data features into a risk feature. The functions $\rho : DF^k \times RF \rightarrow \rm I\!R$ and $\rho^* : DF^k \times RF^n \rightarrow \rm I\!R$ quantify the *local risk* captured by a risk feature and the *overall risk* across all the n risk features, respectively, for each system unit. The calculation of the overall risk via ρ^* is generally governed by a Fuzzy Inference System (FIS) and its underlying fuzzy rule base, as shown in [7], to obtain an interpretable inference process.

When the risk model refers to a particular situational element (e.g., congested traffic lane, piracy attack, vessel moored at port, etc.), we refer to it as an *atomic risk model*. To represent a situation, multiple atomic risk models might be simultaneously at play.

Figure 1 depicts the architecture of the proposed Context-Aware Risk Management Framework (CARMF) that builds upon the blueprint in [8]. The most important element within this diagram is the addition of the *Contextual Knowledge Base* (CKB). The CKB contains information such as regional weather reports, past incidents, operational procedures and guidelines, organizational policies, history of successful responses to events, etc. By making contextual information available to the system, we are able to provide more situation-specific risk assessments and generate responses by integrating that information with the hard and soft sources that are already ingested. The CKB feeds into two modules in the CARMF: the *Dynamic Risk Assessment Module* (DRAM) and the *Contextual Response Filter*.

The Contextual Response Filter will allow the system to remove potential solutions from further consideration based

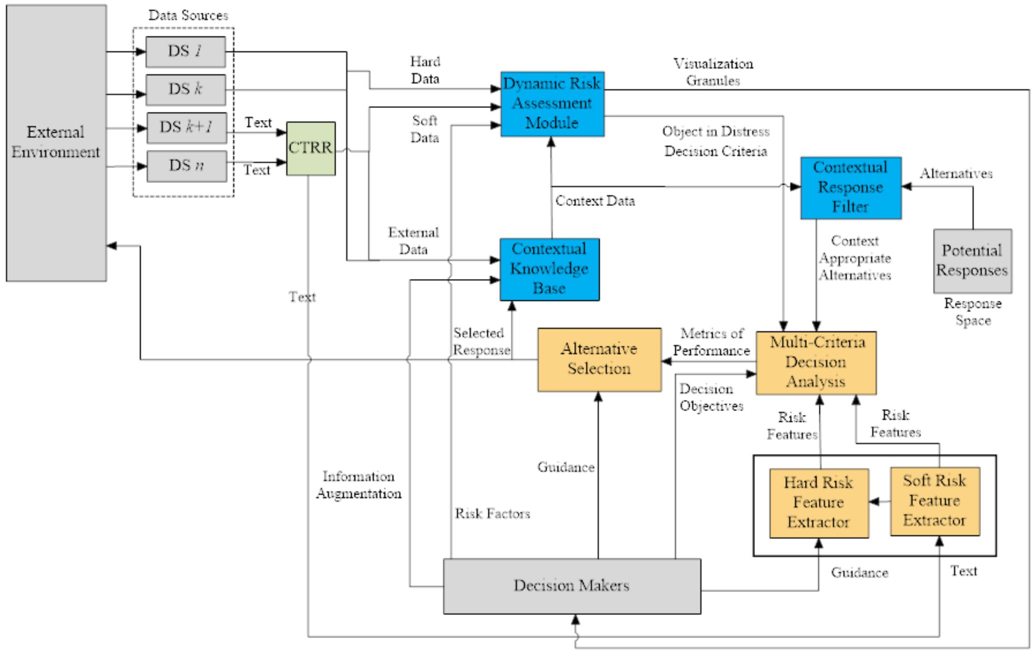

Fig. 1. The RMF's architectural blueprint showcasing modules in both the object and response spaces. Gray boxes indicate external RMF elements. Blue boxes indicate context-related elements. Green boxes indicate Level 2 RMF capabilities and yellow boxes indicate Level 3 RMF capabilities.

on context-specific situational information, such as previous responses to similar scenarios, availability of resources, current conditions, etc. By reducing the number of possible alternatives (i.e., potential responses), we cause the Multi-Criteria Decision Analysis module to require less computational effort as there are fewer candidate solutions for it to evaluate.

The DRAM enables the system to apply only contextually relevant risk models to a given situation. Instead of creating a holistic, static risk model that contains the information about all relevant situational elements, the system will dynamically build a composite model based on a set of local *atomic risk models*, each corresponding to a situational element, to accurately depict the scenario using only the information needed at any point in time.

The DRAM is shown in more detail in Figure 2. Notice that the contextual information is ingested by two sub-modules: *Risk Model Selection* and *Risk Model Adjustment*. The former determines which atomic risk models will be used to represent the current situation given the current contextual knowledge. The list of required atomic risk models is then passed on to the hard and soft risk feature extractors, so that only the required risk features for these risk models are extracted from the raw data stream. The atomic risk models are also conveyed to the *Risk Model Adjustment* sub-module, which employs contextual information in order to tailor the internal risk assessment of these models. For instance Section IV-B unveils an atomic risk model for active weather scenarios. When we apply this risk model, the risk assessment for most of the vessels will be guided by the same set of conditions; however, sailing vessels are more vulnerable to active weather than other vessels. In this case, the risk assessment component of that atomic risk model (and in turn, the fuzzy rules that make up its FIS) would be adjusted to better reflect this. We separate these into two different modules in order to reduce the overall number of risk models and improve the ability for an end-user to properly understand the composite risk models.

The remainder of the CARMF modules retain their original functionality as described in [5], [6], and [8]. In the next section, we illustrate how the DRAM ingests contextual information and exploits it to generate composite risk models based on the list of available atomic risk models.

IV. Case Study: Maritime Risk Assessment

This Section illustrates the application of the DRAM integrating contextual information within two maritime scenarios.

The DRAM uses a set of predefined atomic risk models in order to determine whether or not a maritime vessel is at risk at any point in time. These risk models need not be independent of each other. We can potentially apply multiple risk models to one situation in order to determine the overall risk based on a combination of these models. In this case, it would make sense to have an overall risk equation as follows:

$$\text{if } R_1 \text{ is } HIGH \text{ or } R_2 \text{ is } HIGH \text{ or ... or } R_n \text{ is } HIGH \text{ then } R_{overall} \text{ is } HIGH \quad (1)$$

where R_1, R_2, and R_n are risk models and $R_{overall}$ is the overall reported risk value.

The reason for this is that if we feel a situation warrants more than one risk model (based on contextual risk model activation), then we explicitly care if that model deems there is risk; therefore, if any model indicates risk, the overall model must also indicate risk. Other alternative formulations

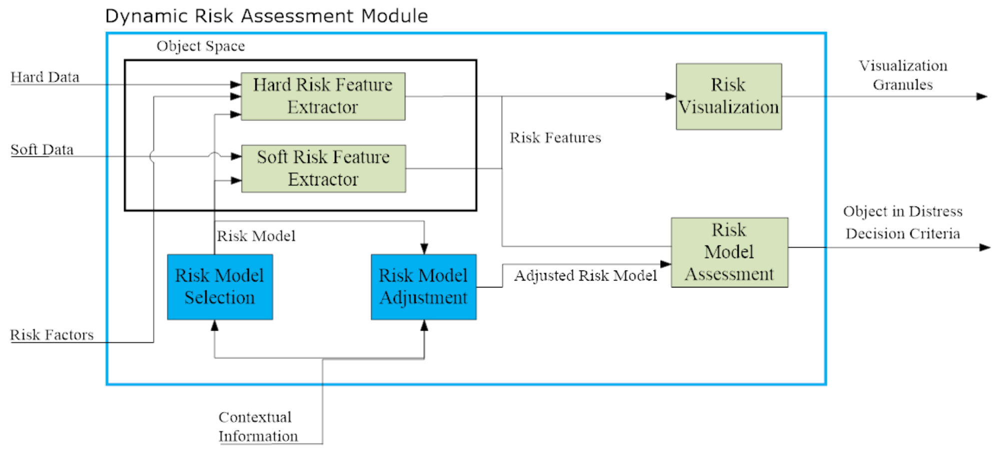

Fig. 2. Architectural blueprint of the Dynamic Risk Assessment module. Green boxes indicate Level 2 RMF capabilities and blue boxes indicate context-related elements.

describing the impact of the local risk models on the overall risk of a system unit could be described via a fuzzy rule base plugged into a well-known Fuzzy Inference System (e.g., Mamdani, Sugeno, etc). Below we introduce the three atomic risk models considered in this work.

A. *Open Water Risk Model*

This is the default model that applies to a vessel when navigating. Its main purpose is to identify the risk of collision with other static (oil rigs, sandbars, etc.) or dynamic (vessels) maritime elements. This acts at the default model because these are factors that can create risk for a vessel at any point in time, not just when under special circumstances. Table I lists the risk features associated with this atomic risk model. In the last column, A, B, C and D refer to the parameters of the trapezoidal membership functions that model the fuzzy sets. These values have been determined using domain knowledge.

In order to capture certain risk scenarios within the risk model, we implement composite risk features that are modeled as weighted sums of the set of atomic risk features extracted from the raw data. These weights represent the individual contribution of each atomic risk feature to the composite risk feature. Their values are determined after consultation with the domain experts. The composite risk features pertaining to the Open Water risk model are shown below:

$$R_{collision} = 0.5R_{proximity} + 0.3R_{seastate} + 0.2R_{speed} \quad (2)$$

$$R_{aground} = 0.4R_{wreck} + 0.3R_{visibility} + 0.3R_{speed} \quad (3)$$

where $R_{collision}$ and $R_{aground}$ are the risk features representing the risk of colliding with another vessel and running into a maritime landmark respectively.

Using the available risk features we create a set of rules to determine the overall risk captured by a model. The fuzzy rule base for the *Open Water* risk model is as follows:

$$\begin{aligned} &\text{if } R_{collision} \text{ is } HIGH \text{ or } R_{aground} \text{ is } HIGH \\ &\qquad\qquad \text{then } R_{open} \text{ is } HIGH \end{aligned} \quad (4)$$

where R_{open} is the overall risk for the *Open Water* risk model.

B. *Active Weather Risk Model*

This model would be applied using regional weather reports to determine if a vessel is in an area where active weather is taking place. This model is applied to take into account that in these situations, vessels are more prone to actions that cannot be controlled or predicted by its crew. This model aims to identify risk of collision due to the challenges that arise from navigating a vessel in an active weather situation.

The Active Weather risk model uses the same risk features as the Open Water risk model, shown in Table I, and the composite risk features seen in Equations (2) and (3). The rule for this model is:

$$\begin{aligned} &\text{if } (R_{collision} \text{ is } HIGH \text{ and } R_{seastate} \text{ is } HIGH) \\ &\text{or } (R_{aground} \text{ is } HIGH \text{ and } R_{seastate} \text{ is } HIGH) \\ &\qquad\qquad \text{then } R_{active} \text{ is } HIGH \end{aligned} \quad (5)$$

where R_{active} is the overall risk for the Active Weather risk model.

This model can also be adjusted by the Risk Model Adjustment module. When the vessel being evaluated is a sailing vessel we change the rule to be the following:

$$\begin{aligned} &\text{if } (R_{collision} \text{ is } HIGH \text{ and } R_{seastate} \text{ is } HIGH) \\ &\text{or } (R_{aground} \text{ is } HIGH \text{ and } R_{seastate} \text{ is } HIGH) \\ &\qquad\qquad \text{or } R_{seastate} \text{ is } HIGH \\ &\qquad\qquad \text{then } R_{active} \text{ is } HIGH \end{aligned} \quad (6)$$

This is added because sailing vessels are more likely to capsize in rough waters. We update the risk model to account for that. It could be argued that we could formulate an entire risk model for this specific scenario, but the idea is to minimize the number of risk models required as they can be difficult to develop whereas adjusting an existing model is much simpler.

C. *Piracy Risk Model*

This model would be triggered when a vessel enters into an area deemed to be at a risk of piracy. These areas could be determined using the regional hostility metric that is described

TABLE I
RISK FEATURES FOR OPEN WATER RISK MODEL

Raw Feature	Risk Feature	Modelling Construct	Parameters/Expression
Vessel Speed (kn)	High Speed Risk([0;1])	Fuzzy set with L-function	A = 5 B = 25
Distance to closest neighbour (m)	High Collision Risk ([0;1])	Fuzzy set with R-function	C = 50 D = 2000
Distance to maritime landmark (m)	High Shipwreck Risk ([0;1])	Fuzzy set with R-function	C = 250 D = 2500
Visibility (km)	High Poor Visibility Risk ([0;1])	Fuzzy set with R-function	C = 1 D = 10
Sea State (Douglas Sea Scale)	High Sea State Risk([0;1])	Nominal Relationship	Calm: Risk = 0 Smooth: Risk = 0.1 Slight: Risk = 0.2 Moderate: Risk = 0.4 Rough: Risk = 0.6 Very Rough: Risk = 0.8 High: Risk = 0.9 Very High: Risk = 1.0

in [8]. The calculation of this metric relies on both hard (AIS messages) and soft (maritime incident reports) data sources. When this metric reaches a certain threshold for a vessel, this risk model could be applied to it. The list of risk features for this atomic risk model is found in Table II whereas its set of composite risk features are given below:

$$R_{boarding1} = 0.15R_{speed} + 0.6R_{proximity} + 0.25R_{swarming} \tag{7}$$

$$R_{boarding2} = 0.2R_{speed} + 0.65R_{proximity} + 0.15R_{visibility} \tag{8}$$

Note that the weighting of $R_{boarding1}$ contains $R_{swarming}$ whereas $R_{boarding2}$ contains $R_{visibility}$. The reason for this difference is that we may be concerned about a single vessel approaching in a poor visibility situation when the detection capability for the vessel at risk may be reduced. The rule used for this model is:

$$\begin{aligned} \text{if } R_{boarding1} \text{ is } HIGH \text{ or } R_{boarding2} \text{ is } HIGH \\ \text{then } R_{piracy} \text{ is } HIGH \end{aligned} \tag{9}$$

V. EXPERIMENTAL EVALUATION

In this section we aim to contrast the previous RMF behaviour (one all-encompassing risk model, no context-based activation), which we refer to as the *general risk model*, with the proposed extension, namely a *set of atomic risk models* that are *activated by context*.

For these experiments, the general risk model will be an application of all three atomic risk models detailed in Section IV at all times. While not appropriate for every situation, without the use of contextual information there is no way to discriminate which atomic risk model(s) are better suited to handle a particular situation. For the dynamic risk model we use the Open Water risk model as the default one; this model will always be applied. The other models may be applied as necessary, which will be explicitly stated in the case studies below. Additionally, in certain cases we can make adjustments to specific risk modules, based on contextual information, in order to make them more applicable to a given situation. Any risk model adjustments that come into play will also be mentioned as they become relevant. For the experiments, we used a HIGH risk threshold of 0.85 and a mean of maximum (MeOM) defuzzifier for our rules.

A. Data Sources

The two scenarios described in Sections V-B and V-C originate from two real-world *textual reports* provided by two reputable sources, namely the International Maritime Organization (IMO) and the Transportation Safety Board of Canada (TSBC). The *positional* and *weather data* for the vessels and the region under consideration are synthetically generated. The *piracy reports* used in the calculation of the regional hostility metric in Section V-B come from the International Maritime Bureau (IMB)'s Piracy Reporting Centre[2]. The raw data that emanates from these data sources are ingested, as shown in Fig. 2, by the RMF's hard and soft risk feature extractors.

B. Scenario 1: Act of Piracy

We simulate a piracy scenario using an actual piracy report from the IMO[3]. The report describes a piracy event that occurred to an underway cargo vessel in the Singapore Strait. Upon passing to the east of Singapore, the cargo vessel is set upon by a pirate vessel, boarded and robbed. By creating a simulation based on this event, we aim to demonstrate the usefulness of having not only a risk assessment being done on the situation on the basis of a static risk model, but the added benefit of having a dynamic, context-based risk assessment.

To this end we examine the track of a vessel moving into a region of known piracy. We use a *regional hostility metric* [8] to determine when the piracy risk model should be applied (for the context-aware approach). The green points in Figure 3 indicate the locations at which we examine the risk models being applied to the cargo vessel. The red points denote the locations of previous piracy events that have taken place in the region. The red point labelled "incident" denotes the location

[2]https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-report
[3]http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Reports/Pages/Default.aspx

TABLE II
RISK FEATURES FOR PIRACY RISK MODEL

Raw Feature	Risk Feature	Modelling Construct	Parameters/ Expression
Vessel Speed (kn)	High 'Speed Too Low' (STL) Risk([0;1])	Fuzzy set with R-function	C = 10 D = 20
Distance to closest neighbour (m)	High Collision Risk ([0;1])	Fuzzy set with R-function	C = 50 D = 3000
Vessels in Proximity (within 2km)	High Swarming Risk ([0;1])	Fuzzy set with L-function	A = 0 B = 1.6
Visibility (km)	High Poor Visibility Risk ([0;1])	Fuzzy set with R-function	C = 1 D = 10

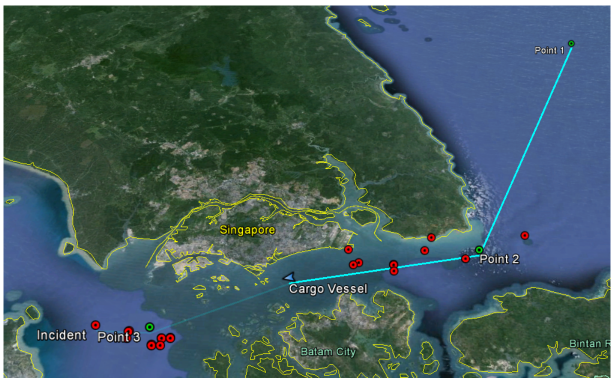

Fig. 3. The path taken by the simulated vessel including the ten closest piracy incidents to each point.

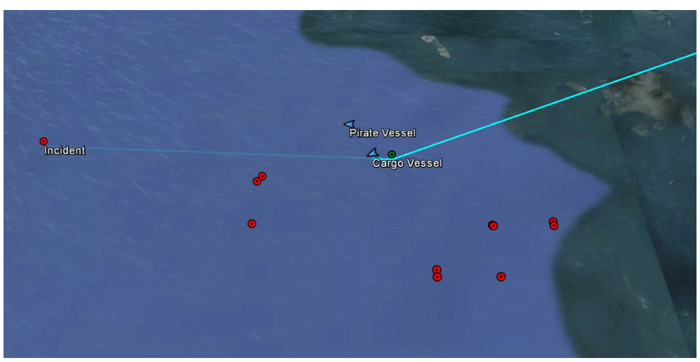

Fig. 4. The simulated cargo vessel being approached by a pirate vessel near Point 3. Includes the ten closest recorded piracy incidents to Point 3.

of the actual piracy event used as the basis for this case study. These piracy events are used to calculate the regional hostility metric and trigger the piracy risk model. Point 1 indicates a location where the vessel is only affected by the Open Water risk model as there is no contextual information that triggers a change in the risk models governing the vessel's risk assessment. Point 2 is where the vessel in question exceeds the user-permissible regional hostility metric threshold –cautiously set at a value of 0.65– and the Piracy risk model comes into play from that point on. Point 3 indicates a moment shortly before the occurrence of a piracy incident.

Figure 4 illustrates the beginning of the piracy event that will take place at the red indicator labelled "incident". Here we show the position of the cargo vessel and the pirate vessel that will attack it. We can also see more closely the location of the previous piracy events that are used to determine the value of the regional hostility metric for Point 3.

TABLE III
RISK FEATURE VALUES FOR THE PIRACY SCENARIO

Risk Feature	Point 1	Point 2	Point 3
High "Speed Too Low" Risk	0.500	0.800	0.900
High Speed Risk	0.286	0.200	0.171
High Proximity Risk	0	0	0.763
High Wreck Risk	0	0	0
High Swarming Risk	0	0	0.625
High Poor Visibility Risk	0	0	0
High Sea State Risk	0	0	0
High Collision Composite Risk	0.057	0.04	0.355
High Aground Composite Risk	0.086	0.06	0.051
High Boarding 1 Composite Risk	0.075	0.120	0.749
High Boarding 2 Composite Risk	0.1	0.160	0.676

TABLE IV
OVERALL RISK VALUES FOR THE PIRACY SCENARIO

Risk Model	**Point 1**	**Point 2**	**Point 3**
Open Water	0.5425	0.53	0.6775
Active Weather	0	0	0
Piracy	0.55	0.58	0.875
Overall (General)	0.55	0.58	0.875
Overall (Dynamic)	0.5425	0.58	0.875

Tables III and IV respectively display the local and overall risk assessment for the atomic risk models in the piracy scenario. At Point 1 the dynamic risk model reports a smaller risk value than the general model. This is because at that point in time the Open Water risk model is the only contextually appropriate model for the dynamic model whereas the general model always includes all models and due to the vessel's low speed the Piracy risk model is evaluated at 0.55, which is an inappropriate level of risk given the vessel's situation at that point in time. At Points 2 and 3, the Piracy risk model is included in the dynamic model, thus causing both the general and dynamic models to arrive at the same overall risk value. It is worth noting that the general model must also calculate the value of the Active Weather risk model even though there are clear seas and skies. The dynamic model provides the advantage of only evaluating models that are contextually relevant, thus reducing the number of rules that need to be evaluated as well as the number of inputs and data required.

Fig. 5. The path taken by the simulated sailing vessel. The white area represents an area affected by active weather.

C. Scenario 2: Sailing Vessel Capsizing

In this scenario, we examine a sailing vessel moving through an area of active weather. This scenario is inspired by a TSBC report detailing the capsizing of a 57.5m Barbados sailing training yacht off the coast of Brazil[4]. In this scenario, the vessel moves into an area of active weather and triggers the Active Weather risk model. This model is triggered using information extracted from soft data sources, i.e. weather reports, to determine which geographical areas are currently experiencing active weather patterns, such as: a thunderstorm, hurricane, typhoon, heavy rains, fog, etc. If an area is deemed to be under the effects of an active weather pattern, then the Active Weather risk model will be applied to any vessel entering that area until the phenomemon has subsided.

In Figure 5, we illustrate the synthetic scenario used to test our risk models. Point 1 is located in open water, free of any active weather patterns. At Point 2 the vessel has entered an area of active weather and the Active Weather risk model is triggered. Since the vessel in question is a sailing vessel, we will apply the adjustment to the Active Weather risk model shown in Section IV-B. Finally at Point 3 the vessel is dealing with the effects of active weather. The red point indicates where the actual capsizing event occurred. In addition to the comparison of the general risk model and the dynamic risk models, we also examine the results of the general model that does not incorporate the risk model adjustment module.

Tables V and VI respectively list the local and overall risk values attained by each atomic risk model in the active weather scenario. In this case study, there is a similar effect on Point 1 as in the previous case study. Here we see that the Piracy risk model is expressing some amount of risk due to low speed, but in this instance lower speeds can even be expected as the vessel in question is a sailing vessel. At Point 2, the Active Weather risk model is triggered by information from weather reports and applied to the dynamic model. In this instance the Active Weather risk model also undergoes an adjustment as described in Section IV-B. At that point the unadjusted and adjusted Active Weather models give the same risk values with the general model still being dominated by the Piracy risk model. Note that this is an area of the world with no reported piracy. At Point 3, we see that the general and dynamic models are both reporting the same level of risk based on the Active Weather risk model. The dynamic model in which the Active Weather risk model adjustment applied shows a much higher level of risk, enough to indicate a risky situation for the vessel. In the report that this case study is based on, the vessel in question capsized and was lost, therefore a risk value indicating a risky situation is not only appropriate, but also expected.

[4]http://www.tsb.gc.ca/eng/rapports-reports/marine/2010/m10f0003/m10f0003.asp

TABLE V
RISK FEATURE VALUES FOR THE ACTIVE WEATHER SCENARIO

Risk Feature	Point 1	Point 2	Point 3
High “Speed Too Low” Risk	0.500	0.800	0.900
High Speed Risk	0.314	0.200	0.171
High Proximity Risk	0	0	0
High Wreck Risk	0	0	0
High Swarming Risk	0	0	0
High Poor Visibility Risk	0	0.222	0.556
High Sea State Risk	0	0.100	0.800
High Collision Composite Risk	0.063	0.23	0.274
High Aground Composite Risk	0.094	0.367	0.218
High Boarding 1 Composite Risk	0.075	0.120	0.135
High Boarding 2 Composite Risk	0.100	0.243	0.263

TABLE VI
OVERALL RISK VALUES FOR THE ACTIVE WEATHER SCENARIO

Risk Model	**Point 1**	**Point 2**	**Point 3**
Open Water	0.5475	0.5625	0.6375
Active Weather	0	0.55	0.7325
Active Weather (adjusted)	0	0.55	0.9
Piracy	0.55	0.6225	0.6325
Overall (General)	0.55	0.6225	0.7325
Overall (Dynamic - Unadjusted)	0.5475	0.5625	0.7325
Overall (Dynamic - Adjusted)	0.5475	0.5625	0.9

VI. CONCLUSIONS

Context-aware information fusion [23] [24] is one of the main research trends within the data/information fusion community given the plethora of contextual data sources available nowadays and the tangible benefits they provide to any fusion process. This paper has brought contextual information to the core of an existing RMF [5] [6] and hence, made it available to any DSS. A Dynamic Risk Assessment Module is proposed to host and coordinate the activation of one or more a-priori-defined atomic risk models guided by context-specific insights drawn from the CKB, or adjusting their internal risk assessment valuations.

The proposed methodology has been illustrated in the maritime domain by means of an act of piracy and an active weather scenario, respectively. The advantages of this RMF augmentation come along four distinct lines: (1) *increased situational understanding*, since each atomic risk model is now subject to an individual risk assessment based on its own set of risk features, therefore equipping the system with

TABLE VII
INTERPRETABILITY METRICS OF THE DIFFERENT RISK MODELS

		Act of Piracy Scenario			Active Weather Scenario		
		Point 1	Point 2	Point 3	Point 1	Point 2	Point 3
General Model	Number of Rules	3	3	3	3	3	3
	Total Rule Length	23	23	23	23	23	23
	Number of Inputs	7	7	7	7	7	7
Dynamic Model	Number of Rules	1	2	2	1	2	2
	Total Rule Length	7	14	14	7	16	16
	Number of Inputs	5	7	7	5	6	6
Dynamic Model (adjusted)	Number of Rules	-	-	-	1	2	2
	Total Rule Length	-	-	-	7	17	17
	Number of Inputs	-	-	-	5	6	6

the ability to track the individual risk contributions made by each risk model to an unfolding situation in the monitoring region; (2) *more interpretable decisions*, as demonstrated in Table VII by the fewer number of rules, their input variables and antecedents in the dynamic risk models compared to the general, self-contained static risk model; (3) *improved support to other fusion tasks* (e.g., intent/threat assessment) within the same fusion process given the modularized nature of the risk derivations; and (4) although perhaps negligible in the two previous case studies, we noticed a *reduced computational effort* due to the fact that only a subset of all atomic risk models need to be loaded and evaluated at any point in time. This aspect gains more prominence as the number of atomic risk models in the system becomes considerably large.

Future work will be geared towards the application of the proposed methodolody to other domains and the exploitation of different types of contextual knowledge as part of the RMF inference mechanism.

REFERENCES

[1] K. Kambatla, G. Kollias, V. Kumar, and A. Grama, "Trends in big data analytics," *Journal of Parallel and Distributed Computing*, vol. 74, no. 7, pp. 2561–2573, 2014.

[2] J. P. Shim, M. Warkentin, J. F. Courtney, D. J. Power, R. Sharda, and C. Carlsson, "Past, present, and future of decision support technology," *Decision support systems*, vol. 33, no. 2, pp. 111–126, 2002.

[3] D. Arnott and G. Pervan, "Eight key issues for the decision support systems discipline," *Decision Support Systems*, vol. 44, no. 3, pp. 657–672, 2008.

[4] D. Arnott and G. Pervan, "A critical analysis of decision support systems research," *Journal of information technology*, vol. 20, no. 2, pp. 67–87, 2005.

[5] R. Falcon, R. Abielmona, and A. Nayak, "An evolving risk management framework for wireless sensor networks," in *Proceedings of the 2011 IEEE Int'l Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA)*, pp. 1–6, September 2011.

[6] R. Falcon and R. Abielmona, "A response-aware risk management framework for search-and-rescue operations," in *2012 IEEE Congress on Evolutionary Computation (CEC)*, pp. 1540–1547, June 2012.

[7] J. McCausland, G. Di-Nardo, R. Falcon, R. Abielmona, V. Groza, and E. Petriu, "A proactive risk-aware robotic sensor network for critical infrastructure protection," in *2013 IEEE Int'l Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, pp. 132–137, July 2013.

[8] R. Falcon, R. Abielmona, S. Billings, A. Plachkov, and H. Abbass, "Risk management with hard-soft data fusion in maritime domain awareness," in *the 2014 Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pp. 1–8, 2014.

[9] R. Falcon, R. Abielmona, and S. Billings, "Risk-driven intent assessment and response generation in maritime surveillance operations," in *2015 IEEE Int'l Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, March 2015.

[10] X. Tan, Y. Zhang, X. Cui, and H. Xi, "Using Hidden Markov Models to evaluate the real-time risks of network," in *Proceedings of IEEE Intl Symposium on Knowledge Acquisition and Modeling Workshop*, pp. 490–493, December 2008.

[11] K. Haslum and A. Arnes, "Real-time risk assessment using continuous-time Hidden Markov Models," in *Proceedings of Intl Conference on Computational Intelligence and Security*, pp. 1536–1540, November 2006.

[12] J. Merrick, J. van Dorp, and V. Dinesh, "Assessing uncertainty in simulation based maritime risk assessment," *Risk Analysis*, vol. 25, pp. 731–743, July 2005.

[13] H. Abbass, A. Bender, S. Gaidow, and P. Whitbread, "Computational red teaming: Past, present and future," *IEEE Computational Intelligence Magazine*, vol. 6, pp. 30–42, February 2011.

[14] A. Yang, H. Abbass, and R. Sarker, "Characterizing warfare in red teaming," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 36, no. 2, pp. 268–285, 2006.

[15] M. Jakob, O. Vanek, S. Urban, P. Benda, and M. Pechoucek, "Adversarial modeling and reasoning in the maritime domain - first year report," *Agent Technology Center, Department of Cybernetics, FEE Czech Technical University in Prague*, 2009.

[16] N. Friedman, *The Naval Institute Guide to World Naval Weapon Systems*. Naval Institute Press, 2006.

[17] I. Lim and F. Jau, "Comprehensive maritime domain awareness: an idea whose time has come?," *Defence, Terrorism and Security, Globalisation and International Trade*, October 2007.

[18] K. Moore, "Predictive analysis for naval deployment activities," *PANDA BAA*, no. 05-44, 2005.

[19] A. H. Razavi, D. Inkpen, R. Falcon, and R. Abielmona, "Textual risk mining for maritime situational awareness," in *2014 IEEE Int'l Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 167–173, March 2014.

[20] A. Plachkov, R. Abielmona, M. Harb, R. Falcon, D. Inkpen, V. Groza, and E. Petriu, "Automatic course of action generation using soft data for maritime domain awareness," in *Proceedings of the 2016 Genetic and Evolutionary Computation Conference Companion*, pp. 1071–1078, ACM, 2016.

[21] J. García, J. Gómez-Romero, M. A. Patricio, J. M. Molina, and G. Rogova, "On the representation and exploitation of context knowledge in a harbor surveillance scenario," in *Information Fusion (FUSION), 2011 Proceedings of the 14th Int'l Conference on*, pp. 1–8, IEEE, 2011.

[22] J. Garcia, J. M. Molina, T. Singh, J. Crassidis, and J. Llinas, "Research opportunities in contextualized fusion systems. the harbor surveillance case," in *International Work-Conference on Artificial Neural Networks*, pp. 621–628, Springer, 2011.

[23] L. Snidaro, J. García, and J. Llinas, "Context-based information fusion: a survey and discussion," *Information Fusion*, vol. 25, pp. 16–31, 2015.

[24] L. Snidaro, J. Garcia-Herrera, J. Llinas, and E. Blasch, *Context-Enhanced Information Fusion*. Springer, 2016.