INMOTOS: Extending the ROPE-methodology

Lorenz Zechner
SBA Research
Vienna, Austria
lzechner@sba-research.org

Peter Kieseberg
SBA Research
Vienna, Austria
pkieseberg@sba-research.org

Edgar Weippl
SBA Research
Vienna, Austria
eweippl@sba-research.org

ABSTRACT

The Interdependency Modeling Tool and Simulation (INMOTOS) project is aimed to develop a tool for modeling and assessment of interdependent business- and contingency plans and risks affecting them. In the scope of that project a methodology had to be created that enables the modeling of highly complex business processes, their structures and interdependencies, as well as threats and countermeasures. A time-based simulation of the impact of possible threats is required as well as a risk assessment by using multiple different impact calculations. The methodology shall be kept simple and flexible to enable modeling of a wide range of different business scenarios. For the fundamental basics the Risk-Oriented Process Evaluation (ROPE) methodology [7] was chosen due to its high flexibility. This paper describes the adaptations and enhancements that are applied on the ROPE methodology to refine it to the INMOTOS methodology.

Categories and Subject Descriptors

I.6.5 [**Model Development**]: Modeling methodologies; I.6.8 [**Types of Simulation**]: Combined

General Terms

risk assessment, methodology, contingency plans, interdependent business processes

1. INTRODUCTION

In the modern age, it is noticeable that business processes in companies tend to become more and more complicated. Furthermore the globalization effects companies in many ways and is causing them to rely on the supply of resources, infrastructure or know-how from other companies, often located at the other end of the world. Hence, disasters striking in far-away locations can heavily influence production chains and business processes of companies all over the world. Thus, it is not feasible anymore to assess only company-internal business processes and contingency plans, interdependencies between the business processes of multiple companies have to be modeled and their impact analyzed during risk assessment. Furthermore, one single way to evaluate risks is not sufficient in many cases[2]. Risks have to be evaluated based on multiple approaches, values and perspectives. This is where the INMOTOS methodology comes into play. The goal is to create a tool for dynamic risk assessment that enables the modeling of interdependencies between several companies, to model risks affecting the business processes and to evaluate the contingency plans the companies have in place concerning their effectiveness, completeness and reliability. This work presents such a methodology by using an existing methodology (ROPE) for the fundamental basics and enhancing it to fulfill the operational, logical and technological requirements of the INMOTOS project.

iiWAS2012, 3-5 December, 2012, Bali, Indonesia.

2. RELATED WORK

2.1 The ROPE methodology

The ROPE (Risk-Oriented Process Evaluation) - Methodology introduced by Jakoubi et.al. in [7] is aimed to provide a practical and comprehensive tool for combining the capabilities of business process management, business continuity management and risk management. It is designed for holistic evaluations of business processes together with the risks and their resulting costs, as well as the long-term effects. The practical applicability was for example demonstrated in [13], where ROPE was used to enhance business continuity management in the case of natural disasters or criminal attacks. ROPE uses three layers for describing business processes and the risks they are exposed to, together with the resulting effects in case a risk becomes reality:

- The Business Process Modeling (BPM) layer: This layer represents the business processes.
- The Condition, Action, Resource and Environments (CARE) modeling layer: In this layer, the underlying elements (e.g. actions, resources and environments) of the business processes are identified, defined and modeled as elements of the overall model.
- The Threat Impact Process (TIP) modeling layer: This layer is used for identification and modeling of potential threats, but also eventual countermeasures and recovery strategies.

2.2 Alternative methodologies

In [6] Jakoubi et.al. compared nine different research approaches towards integration of security and risk aspects into business process management and identified future challenges for research. Additionally in [5] Jakoubi et.al. show an approach to derive resource requirements and apply them to risk aware business process modeling. In [12] Taylor et.al. show the creation of a new risk assessment approach specialized on the oil and gas sector and focused on the region of the gulf of Thailand. In [10] Olita et.al. created a risk assessment for oil spills, showing dispersal of the oil on sea and at shores In [11] Orme and Venturini present a risk assessment approach using multiple separate parameters for risk evaluation. In [9] Miri Lavasani et.al. introduced an approach for a hierarchical analytical process for risk assessment, which is focused on an easy update with newly gathered information. In [3] Chen, Chen and Li introduced an approach to assess risks during an occurring incident, which is essential knowledge for a time based risk assessment. [1] Aven analyzed the problem of finding methods to objectively assess human lives claimed and damage done to the environment in a risk assessment methodology. In [4] Fedeski et.al. and [8] Klein et.al. did both show approaches for risk assessment taking environmental factors into consideration. Additionally in course of the INMOTOS project a study was made to compare 31 standards, guidelines and methodologies with the requirements of the project.

3. PROBLEM DESCRIPTION

3.1 The INMOTOS Project

Today companies face the problem that critical infrastructure is often affected by threats that (can) handicap or disrupt their workflow causing high financial costs or, in the worst case, claim human life. Most companies have contingency plans ready at hand in case such a disaster strikes. The feasibility of these contingency plans is often unknown and untested, contingency plans of other companies might interfere with own contingency plans or even with the daily business processes. This fact is frequently unaccounted by companies so that in case a disaster strikes these companies are blindsided or surprised. It is the goal of the INMOTOS project [2] to create a tool, that enables companies to validate and assess their business processes as well as the occurring risks and especially their contingency plans. The primary goal of the tool is to enable users to model business processes, their functionality and requirements, their impact on each other and to assess contingency plans that are in place at the companies. Also, based on these business processes, possible threats and their impact on the overall picture shall be modeled and evaluated. The interdependency of business processes and contingency plans and possible influences on each other play a key role in the project and received special attention during the development of the methodology. As basis for this methodology ROPE [7] was chosen due to its adaptivity. Due to its modular design, new states and concepts can be added and existing ones can be altered to meet new conditions. Also ROPE offered, already beginning from its original state, a wide variety of attributes required by INMOTOS which made it an ideal starting point for the INMOTOS methodology.

3.2 Requirements encountered during the INMOTOS project

ROPE	Requirement
	Interdependency between contingency plans
X	Timebased processing
X	Connection between Elements
X	Detailed Threat Modeling
	Detailed Modeling of contingency plans
	Modeling of complex inter-business scenarios
X	Determination of capacities of resources
X	Risk assessment by revenue loss and gain
	Risk assessment by SLAs
	Risk assessment by life claimed
	Risk assessment by individual parameter

Table 1: ROPE compared to the INMOTOS requirements

Business processes have to be modeled in a very simple but powerful way that enables high flexibility and adaptivity during simulation. Altogether the following main requirements for the INMOTOS methodology were identified:

- **Interdependency** between business processes and contingency plans of different companies
- **Time based flow - simulation** has to be possible
- **Connections** between all relevant elements of the methodology
- **Threats** and their results modeled in high detail
- **Complex scenarios** convertible in the methodology
- **Countermeasures** and their relation to resources and following business processes convertible in the methodology
- **Capacities of resources** modeled and their development be traced over time
- Risk assessment based on **revenue losses and gains**
- Risk assessment based on **existing contracts and their Service Level Agreements (SLA)** and if they can be kept
- Risk assessment based on **human life claimed** due to threats occurring and countermeasures being triggered
- Risk assessment of **individual parameters** of the participating companies shall be possible

As shown in table 1 the ROPE methodology offers great potential from the start, but several important requirements from the INMOTOS project are not yet satisfied. The following chapter 4 will describe, which adaptation and new developments to the ROPE methodology had to be done.

4. EXTENSIONS TO THE METHODOLOGY

4.1 Agents

In order to adapt the ROPE methodology to the INMOTOS requirements, interdependent contingency plans have to be representable. In the course of the project several real-life contingency plan were assessed and it was soon realized that the agents available in ROPE are not sufficient to model current counter-strategies. Especially, the strategy of switching to alternative resources is impossible to model. Since this switch is likely to interfere with business plans of other companies, analysis of such interdependencies is of high importance. This led to the inclusion of a separate agent in the model for this scenario. The agent (see Figure 1) basically models the switch from one resource to another and the costs related to this. Table 2 gives an

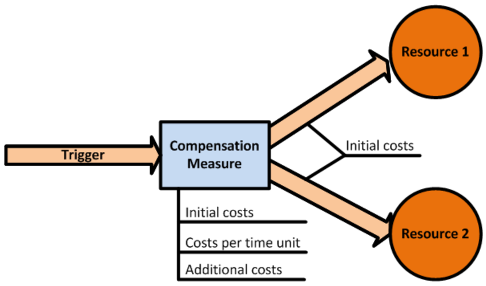

Figure 1: Example of the Compensation Measure Agent

Attribute	Definition
Initial costs	One-time costs to set up the restoration measure
Costs per time unit	Costs per time unit to perform the restoration measure
Additional costs	Additional costs due to different price per unit of the substituted resource

Table 2: List of Attributes of the Compensation Measure Agent

overview on the attributes of this agent.

Additionally, a special connector was established that connects the Compensation Measure Agent to the resources that shall be switched. The connector itself also holds information on how much capacity of the new resource is required in case the old resource can still be used partially.
Furthermore, the resource agent had to undergo severe changes. The resources needed to be split up into 6 resource types, each with an agent of its own, to model the resources unique attributes and parameters (see Table 3).

Flexibility was the primary target when designing the resource agents. Thus, every agent is equipped with an individual set of attributes required to model availability, costs, political impact and other attributes. A complete list of all attributes of the agents and their description can be found in chapter 4.3.

Resource	Description
Raw Material	Simulates a source of raw material. Several agents can produce the same raw material
Environment	Stands for environmental resources and conditions that are relevant to the production
Governmental structure	Holds information about resources provided by governmental resource providers.
Security	Models information about security relevant resources.
Employee	Models information about available employees
Infrastructure	Describes infrastructure resources required for an action

Table 3: List of Resources

4.2 Connectors

New connectors need to be added to model occurring threats and the effect of non-successful threat actions in detail. It is important that a threat is not considered isolated, but with all its global connections. This especially means that one threat can (but doesn't have to) trigger other treats. The same goes for countermeasures, especially when they fail. So, for example, a failed attempt to lower gas temperature may cause additional damage to the pipeline. To model such complex threat-countermeasure dependencies, several connectors have been added to the model.

4.3 Attributes

Additionally, attributes were added to enable risk assessment based on complex scenarios and evaluation based on multiple rating schemes. Since the tool created in the IN-MOTOS project is going to use colored petri nets, the methodology can enhance connectors to be containers for complex business logics. Adaptions were made to identify and assess interferences between multiple contingency plans and to enable risk assessment based on several different approaches. All in all the following extensions to the attributes of ROPE were done:

- Service Level Agreements (SLA) and obligations resulting from them
- Service Level Agreements (SLA) and penalties in case of failure to perform
- Available and required capacities were added in multiple agents
- A stock was added to multiple agents
- Responsibilities were added for business processes
- Value for business processes were added
- Costs (one time and over time) were added to multiple agents
- Availability of a resource to multiple companies introduced
- Replenishment rated added to resources
- Revenues due to e.g. granting programs added (one time and over time)
- Maintenance costs added
- Salary costs added
- human casualties added (Public View vs. Private View - see chapter 4.5
- Duration and fade off added to threats and threat actions
- Probability of success and occurrence added to several agents

4.4 Interdependencies

As one of the main requirements of the project, the methodology shall be able to model interdependencies between different contingency plans but also incorporate business plans. Therefore two functionalities had to be included in the IN-MOTOS methodology:

- We added the concept, that basically every resource can also be modeled as a separate business process, which by itself requires resources and is affected by threats. Therefor, by clicking a resource node, its possible to drill down the view to see how a resource is generated and threats affecting a business process also affect companies requiring the output of these business processes.

- Additionally we added a check to model if a resource exceeds its capacity to be able to identify bottlenecks when multiple companies drain one resource without knowing from each other.

4.5 Methods for risk assessment

In the course of the INMOTOS project, several different approaches to assess risks and contingency plans had to be included. A risk evaluation can either be done by starting a simulation and let threats strike by their chance of occurrence or by specifically triggering threats. Furthermore, success or failure of a specific part of the contingency plan can be predefined in the simulation.

4.5.1 *Value*

Value describes a free-to-configure measurement system to assess risks in INMOTOS. "Value" is stored in the business process agent and can hold either a concrete pecuniary equivalent of the value of the business process or a more abstract, company-individual concept of credit model to calculate business processes that generate output that is essential but not measurable in money. The risk assessment itself is based on the "value" field of the business process agent. This value is affected by a series of probabilities modeled in the INMOTOS methodology schemata, e.g. the expected impact of threats based on their occurrence probability, the occurrence probability of certain threat actions and the impact of contingency plans and the impact on running actions and business processes. The result can be written down formally as $C_O \cdot C_A \cdot C_C \cdot C_L \cdot V$, where C_O denotes the chance of threat occurrence, C_A the chance of threat *action* occurrence, C_C the chance of countermeasures failing, C_L the limitation of the business process due to handicapped actions and V the value of the business process.

When this formula is resolved, a concrete number assigning the value of the risk is calculated, no matter if it represents a certain monetary value or a more sophisticated assessment methodology.

4.5.2 *Costs*

Risk assessments by costs are based on the additional costs, penalties, damage, etc. that arise due to the impact of threats and the activated contingency plans. Elements of the INMOTOS methodology that might inflict additional costs possess fields to enter the expected additional costs. This includes fields for one-time costs (e.g. initial costs) as well as regular occurring costs (e.g. upkeep for countermeasures). Also the use of elements like compensation agents can lead to additional costs due to increased costs for the substituted resources. By summing up the additional costs arising and taking into account the probabilities of risks and the success probability of the contingency plan, the additional costs per threat can be calculated.

4.5.3 *Penalties*

The calculation basically corresponds to the calculation of the risk assessment via value, just that instead of the "value" field, the field representing the penalties due to SLA (Service Level Agreement) are used. The formula therefore is similar to the one used to assess risks based on the value.

4.5.4 *Human Life Claimed*

We decided to include only a rough estimation on potential life loss in our model. The calculation of human losses is based on two approaches:

Company view.
The company view only holds information about casualties caused directly by the actions and decisions made by the company.
Most INMOTOS methodology agents in the TIP layer have a separate field to enter expected losses for both, initiation and during runtime per time unit as far as these casualties are caused due to steps taken by the company (e.g. certain countermeasures triggered).

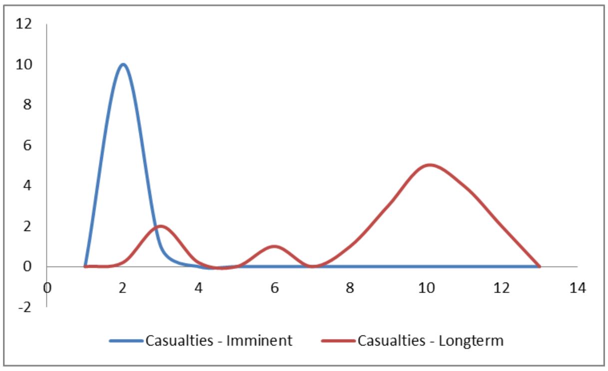

Figure 2: Development of casualties - company view

As can be seen in figure 2, the highest amount of casualties occurs directly after the accident, but the number of long term casualties per time unit have to be taken into account too.
For evaluating risks, either the total potential losses can be considered or average losses due to a threat per time unit.

- Total losses:
  This number represents the total of all losses that would occur due to the expectations and assumptions of the contingency plan during the whole runtime of the threat impact.
- Losses per time unit:
  Here the expected casualties are represented per time unit so that the development of losses can be visualized. This view is designed to visualize risks of long lasting disasters.

Public view.
The public view holds all casualties that a threat causes, no matter if they can be linked directly to any action of a company or not. For example: In case a disaster strikes this value also holds casualties that were caused by the disaster itself and were not caused by actions of company / contingency plan.
Figure 3 shows the difference in a disaster between company view and public view - please keep in mind the different scaling.

5. EVALUATION

5.1 Scenario

In this chapter we will show how to practically apply the INMOTOS methodology for a (simplified) use case scenario.

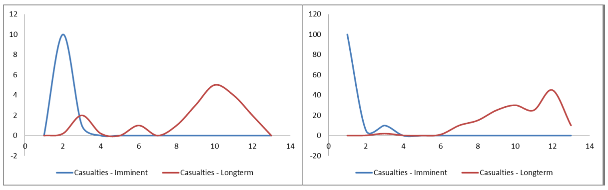

Figure 3: Comparison of Company View and Public View

For the use case we assume a pipeline operator that has to deliver a certain amount of gas due to SLA contracts from country A to country B. The use case is based on a real life example provided to us by the INMOTOS consortium.
The transfer takes place by using two multi-segmented pipelines that run in parallel. Both pipelines are required simultaneously to keep the process running. As soon as one pipeline is down, the second pipeline has to be taken out of operation, too. The company operating the pipelines has installed 2 detection agents, checking if certain threats occur, and also has several contingency plans in place in case disasters strike.

5.2 Resulting Model

5.2.1 BP Layer

As a first step in modeling a scenario in the INMOTOS methodology the business processes that are relevant have to be identified (Figure 4). The business process consists of transporting gas from country A to country B. The company has certain obligations to keep or face a penalty. The field "Value" is used to determine the importance of the business process to the company, in this case holding a monetary value.

5.2.2 CARE Layer

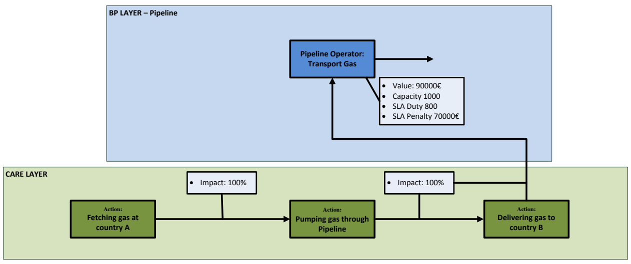

Figure 4: Use Case: CARE Layer - Actions

After the business processes have been modeled in a next step they are broken down in actions that have to be done to complete the business process in an ordinary day to day routine (Figure 4). In this case we use a rather simple scenario of 3 actions being required to fulfil our business process. When one action stops working, all other actions are affected too.

To be able to see if all requirements for an action are fulfilled we have to add the resources needed to complete an action (Figure 5). In this case we have 2 pipelines running parallel each consisting of 2 sections. All sections have a certain capacity and operating-costs, since they are of type "Resource - Installation". A complete list of resource types and their attributes can be found in table 3.

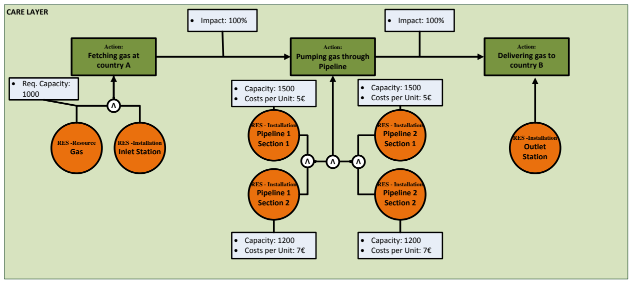

Figure 5: Use Case: CARE Layer - Resources

5.2.3 TIP Layer

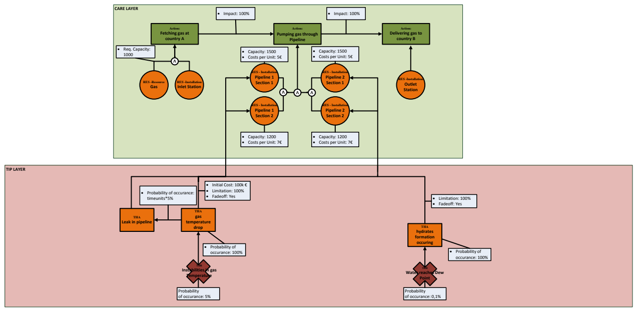

Figure 6: Use Case: TIP Layer - Threats

As a next step we have to add threats and threat actions to the system (Figure 6). If such a threat occurs, it has a certain chance to cause a threat action that can cause initial costs and limit resources. Also a threat action has the chance to cause another threat action (e.g. a too high gas temperature may cause a leak in the pipeline).

To be able to react on occurring threats we need to install detection agents (Figure7). These agents are mechanisms that check if certain threats or threat actions occur and can trigger countermeasures of any kind. In this model it is assumed that detection agents always detect the threats they are meant to detect. After we added the agents to detect

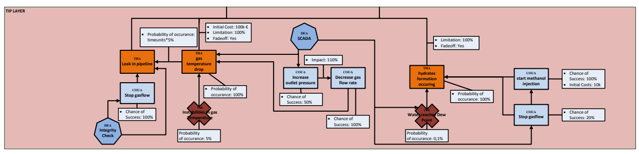

Figure 7: Use Case: TIP Layer - Full Contingency Plan

threats in the last step, we now have to eliminate the threat and its effect on the resources. To model these counter strategies (Figure 7) the INMOTOS methodology offers 3 agent types:

Countermeasure Agent: Countermeasure agents are used to counter a concrete threat or threat action.

Restoration Agent: Restoration agents are used to model approaches to restore resources to their original states.

Compensation Agent: Models (temporary) switches to other resources (see chapter 4.1).

5.3 Future Research

In the future we plan to realize the proposed methodology in a concrete tool in course of the INMOTOS project and to develop a descriptive language to insert not only concrete values in the agents' attributes but also more flexible formulas. The tool will be realized by using colored petri nets in Ruby. The methodology provides enough flexibility to allow for the addition of new agents and attributes in case special requirements ask for this. Still, the current form of the methodology is flexible enough to provide the tools needed for a wide range of different application scenarios.

6. CONCLUSION

In this paper we did show an enhancement to the ROPE methodology to satisfy the requirements of a flexible risk assessment tool to model interdependencies in contingency plans. Nowadays business processes often rely heavily on cooperation between companies that are located far away from each other. Therefore a disaster striking on one side of the world can severely affect companies that are located physically far away. It is therefore of high importance to keep such interdependencies in mind when assessing and modeling risks and countermeasures. Therefore the INMOTOS methodology provides the following enhancements over the original ROPE methodology:

- Simulation of interdependencies between several business processes, be it the mutual use of resources or the allocation of resources
- Assessment of risks using not only costs but also using occurring penalties, importance of the business process and the number of human life claimed
- The TIP layer was heavily adapted to enable the switch to other resources in case of disasters and also to simulate that also counter strategies require certain resources to work
- Enhancing all agents by multiple attributes to improve the simulation of the workflows and impacts within the business processes but keeping the agents still as flexible and general as possible
- Enabling capacity tracking with special focus on identifying bottlenecks when multiple companies drain one resource at the same time
- Extending Connectors to use the possibilities of colored petri nets and holding information by themselves
- Possibility for using formal languages instead of fix values added to multiple attributes

7. ACKNOWLEDGMENTS

The research was funded by COMET K1, FFG - Austrian Research Promotion Agency and grant C2-067 (INMOTOS) by the European Commission.

8. REFERENCES

[1] T. Aven. Selective critique of risk assessments with recommendations for improving methodology and practise. *Reliability Engineering & System Safety*, 2011.

[2] M. Barbieri, I. Cibrario Bertolotti, M. Cheminod, I. Christou, L. Durante, S. Efremidis, G. Gentile, P. Kieseberg, S. Lehmann, P. Paci, M. Pesce, A. Ronge, M. Tanas, C. Taverner, and L. Zechner. Inmotos project. In *Conference on Critical Information Infrastructures Security 2012, CRITIS'12*, 2012.

[3] A. Chen, N. Chen, and J. Li. During-incident process assessment in emergency management: Concept and strategy. *Safety Science*, 2011.

[4] M. Fedeski and J. Gwilliam. Urban sustainability in the presence of flood and geological hazards: The development of a gis-based vulnerability and risk assessment methodology. *Landscape and urban planning*, 83(1):50–61, 2007.

[5] S. Jakoubi, G. Goluch, S. Tjoa, and G. Quirchmayr. Deriving resource requirements applying risk-aware business process modeling and simulation. 2008.

[6] S. Jakoubi, S. Tjoa, G. Goluch, and G. Quirchmayr. A survey of scientific approaches considering the integration of security and risk aspects into business process management. In *Database and Expert Systems Application, 2009. DEXA'09. 20th International Workshop on*, pages 127–132. IEEE, 2009.

[7] S. Jakoubi, S. Tjoa, and G. Quirchmayr. Rope: A methodology for enabling the risk-aware modeling and simulation of business processes. In *ECIS 15th European Conference on Information Systems*, pages 1596–1607. University of St. Gallen, 2007.

[8] B. Klein, A. Schumann, and M. Pahlow. Copulas–new risk assessment methodology for dam safety. *Flood Risk Assessment and Management*, pages 149–185, 2011.

[9] S. Miri Lavasani, Z. Yang, J. Finlay, and J. Wang. Fuzzy risk assessment of oil and gas offshore wells. *Process Safety and Environmental Protection*, 2011.

[10] A. Olita, A. Cucco, S. Simeone, A. Ribotti, L. Fazioli, B. Sorgente, and R. Sorgente. Oil spill hazard and risk assessment for the shorelines of a mediterranean coastal archipelago. *Ocean & Coastal Management*, 2011.

[11] G. Orme and M. Venturini. Property risk assessment for power plants: Methodology, validation and application. *Energy*, 2011.

[12] L. Taylor, J. Suthin, and B. King. Integrated risk assessment and management of oil spills in the gulf of thailand. In *International Petroleum Technology Conference*, 2011.

[13] S. Tjoa, S. Jakoubi, and G. Quirchmayr. Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 179–186. IEEE, 2008.