Cost-Risk Optimization Applied in the Context of Regulation

Ibtissem Chouba[1,2] and Jean-Sébastien Sottet[2]
[1]*Université de Lorraine, France*
[2]*LIST, 5 avenue des Hauts Fourneaux, L- Luxembourg, Luxembourg*

Keywords: Regulation, Optimization, Mixed Integer Linear Program.

Abstract: Most engineering, maintenance and operating decisions involve some aspect of Cost/risk trade-off. In this context we will talk about the cost- risk optimization applied to information systems in the context of application of regulations. In this paper, a conceptual model of risk based regulation, based on the existing business and risk architecture models will be presented. Then, a conceptual cost-risk model associated with the implementation of risk mitigating controls will be adopted and integrated into the optimization approach. Following this cost model, a mixed-integer linear program will be described. The bi-objective optimization of the risk-cost will then be solved with IBM ILOG CPLEX optimizer to define an optimized solution. The result of the calculation of the optimization will serve as a help to the decision-making of the company.

1 INTRODUCTION

Regulation has multiple objectives (stability of the system, access to the market, consumer protection), and is complemented by legal obligations (European regulations and directives) and recommendations of good practices (industrial and international standards). However, responding to regulation is increasingly burdensome for companies, both in terms of financial cost, but also complexity. This cost, in terms of infrastructure, personnel, etc. can be weighed against the level of risk of non-compliance.

Risk-based regulation consists in expressing the regulation in terms of risks to be mitigated. The identification of risks (and related threats) as well as the tolerance level is defined by the authorities (i.e., the regulators). One constraint is that such risk-based regulation should be made at the overall enterprise level, thus based on enterprise models (Lankhorst, Marc M., 2004).

In this context, we rely on a model-driven approach (Barbero, M., et al., 2008; Salay, R., et al., 2009) which relates together multiple models of different nature (enterprise models, risks and threats models, etc.). We then combine, through transformations, this multi-model approach with optimization. As a result, we focus on the cost-risk optimization that the company faces when imposing a new regulation, modifying an existing regulation. We design an optimization approach that will help enterprises' decision makers to select the appropriate costs regarding risk tolerance and enterprise investment capabilities. The example used in this article is based on Information Technologies Security (ITS) risks.

This paper is organized as follow: first we introduce the related work on cost-risk optimization. In Section 3 we introduce our model-based approach used for risk management including enterprise assets, and the threat setting. Section 4 shows our conceptual contribution for cost-risk modelling. Section 5 proposes our technical solutions and practical modelling of the risk-based optimization problem. Section 6 depicts a comparison between the technical solutions implemented. We finally conclude this article in Section 7.

2 RELATED WORK

Optimization is a large field with a lot of domain application. We here focus on a bi-criteria optimisation: risk-cost. One of the peculiarities of our work is to propose a holistic and local view on the enterprise assets (supported by enterprise model) to help decision maker Risk-cost optimization is proposed in different domains, with different approaches (Rocchetta, R., et al., 2015;

Chouba, I. and Sottet, J-S.
Cost-Risk Optimization Applied in the Context of Regulation.
DOI: 10.5220/0006659105360543
In *Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development (MODELSWARD 2018)*, pages 536-543
ISBN: 978-989-758-283-7

Goettelmann, E., et al., 2013; Poolsappasit, N., et al., 2012).

In (Rocchetta, R., et al., 2015), and in the system engineering field, the authors discuss the problem of cost-risk optimization in the context of risk assessment of distributed energy systems considering extreme weather conditions. In this context, a framework for probabilistic risk assessment and a framework for cost-risk optimization using the evolutionary algorithm NSGAII (Deb, K., et al., 2002) were developed.

In the field of industry, many mathematical and heuristic models have been developed with the aim of optimizing the supply chain using the Just In Time (JIT) approach but without taking into consideration the potential risks that may occur during its implementation and cause significant disruption to all members of the supply chain. In (El Dabee, F., et al., 2014), the genetic algorithm is developed to find the optimal solution of the mathematical model proposed in (Medical laboratories AT, 2012), thus reducing the cost-risk of the final product in the JIT production system.

In (Goettelmann, E., et al., 2013) it is to optimize the quality of service (and its cost) to the security risk, helping to choose the right cloud service broker. They used a heuristic approach, based on the Tabu-search algorithm (Glover, F., 1997). Here the approach includes a pre-partitioning of the data.

In (Poolsappasit, N., et al., 2012), inspired by "attack-tree" (Dewri, R., 2007), the authors propose a version based on Bayesian networks to model the probabilities of risk (these are used to reduce optimizing the risk-cost in a system whose resources are limited). Probabilities come from different sources. In addition, they propose the use of a genetic algorithm in order to propose different solutions for mono optimizations (e.g., reduce only the cost) and multi-objectives.

In (Špačková, O., and Straub, D., 2015), the cost-benefit analysis method was studied in the framework of cost-risk optimization under budgetary constraints. This study has been developed within the framework of natural hazard management, but it can be applied to various risk management domains. This method was used to identify risk mitigation strategies by ensuring equivalence between control costs and the reduced value of risks.

In the MDE community a very few work addressed the combination of metamodels and optimization. For instance, in (Dougherty, B., et al., 2012), they use optimisation cloud computing consumption and resources using model-driven configurations – including constraints – and relying on a constraint solver. Early works, focusing on code generation addressed optimization of the generated code but not use optimization and models in a decision process.

3 MULTI-MODELS: ENTERPRISE RISK BASED REGULATION

Risk assessment is one of the mandatory tasks a service provider (i.e., a regulated enterprise) has to do in order to show its compliance with given regulations. The regulation institutes are responsible of the stability are to assess the compliance reports of the enterprises. Regulation institutes are asking regulated enterprises to establish of a homogeneous risk assessment following regulation rules.

Then, as the risk assessment covers all the enterprise assets that are of different nature: people, IT infrastructure, products, services, data, etc. We use Enterprise Architecture Model (Lankhorst, Marc M., 2004; M. Op't Land, et al., 2008) (EAM) for modelling the enterprise assets. EAM provides the necessary abstraction to avoid setting too much modelling element whilst keeping the essence of enterprise business, technical assets and processes. In addition, risk assessment is provided by different information source concerning threats (e.g., threat database, standard threats in a given domain, vulnerability, etc.), controls (i.e, threat mitigation), actual incidents, etc. The regulation institutes are also dealing with models and they need an holistic view on the level of compliance aggregating and consequently comparing the models coming from the regulated enterprise".

In this context, we need to support the various models used in enterprise risk-assessment and relate them together (e.g., vulnerability represents a relation between a threat an EAM element). Technically, we based our approach on a model environment we developed (Sottet, J. S. and Biri, N. (2016). This modelling environment allows for more flexibility when dealing with uncertainty in modelling notably when linking modelling elements.

3.1 Enterprise Architecture Model

EAM (Lankhorst, Marc M., 2004; M. Op't Land, et al., 2008) have been developed to support enterprises governance tasks. They help mastering the complexity of organisation, changes in organisations, facing crisis, etc. They are used in

many situations (A. Anaby-Tavor, 2010): internal communication, strategy and vision development, enterprise transformation, knowledge management, costing, etc.

We use Archimate, the open-group standard to build an EAM. This model is then imported into our environment to be used as a base reference model for the risk assessment.

3.2 Reference Models for Risk Assessments

Risk assessment incorporates risk analysis and risk management, i.e., it combines systematic processes for risk identification and determination of their consequences, and how to deal with these risks.

We build a relation between EAM assets and risk assets in order to propose a reference view on enterprise risk assessment: we map threats and vulnerabilities that impact enterprise assets.

As a first step, a reference EAM is established by regulation body and depicts the typical elements (processes, data, document, personnel, etc.) that an enterprise in a given sector could conform to.

The map between reference architecture and threats could also be given by regulation bodies. They identify which assets is influence by which threat. Figure 1 shows our conceptual view of reference enterprise risk assessment elements. We have put in addition the objectives impacted by the threat (i.e., threat consequences) as well as the control that mitigate the threats. The level of acceptability of a threat regarding an asset is also given by regulation institute.

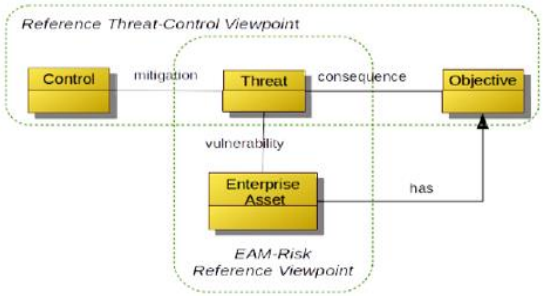

Figure 1: Conceptual metamodel for Risk Assessment.

3.3 Risk Assessment Process

The risk assessment process is mainly a model-based activity: injecting models from different sources in our modelling environment. As a result, the reference architecture model is provided from the Archi environment. A specific injector has been developed for translating Archi models in XMI in our environment that eludes all unnecessary elements for establishing a reference model. The controls and threats models come from different source (threats are defined by some standard body or provided by recurring incident bases). In this first experiment we imported controls and threat from existing tool e.g., (Nicolas Mayer and Jocelyn Aubert, 2014).

We have defined our own process for enterprise risk assessment. First the reference models (threats, controls and architecture) are given by the regulation institute. It stipulates the organisation of risk assessment that a regulated enterprise has to perform. In a second type, the enterprise can personalize the reference model (provide more detailed information).

The main difference regarding traditional approach (Dubois, É., et al., 2010) is that risk assessment is done by providing control on actual threats that impact assets. The relation between threats and enterprise assets is to be given (i.e., we know that a potential intrusion could affect all enterprise's application servers visible on internet).

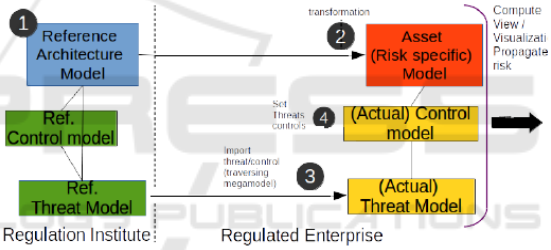

Figure 2: Risk assessment process.

4 CONCEPTUAL COST-RISK MODEL

In order to maintain organization's standard of excellence, it requires solutions to continuously manage operations while striking the right balance between cost optimization, and risk control. For that reason we define the following cost-risk model.

This conceptual cost-risk model was established with the purpose to apply an optimization approach that represents the risk assessment step (step 4 in Figure 2). This step is about setting the controls to mitigate risks.

In Figure 3, we propose a more detailed metamodel of risk assessment for the risk-cost optimization purpose. Compared with the conceptual metamodel of risk assessment in figure 1, the concept of Risk cost, Decision, Maximum cost, residual risk, inherent risk, assets have been added.

Our Cost-Risk metamodel offers objects composed of risk scenarios by asset or group of assets. This modelling facilitates the management of the most common risks and allows gaining in objectivity as well as in efficiency.

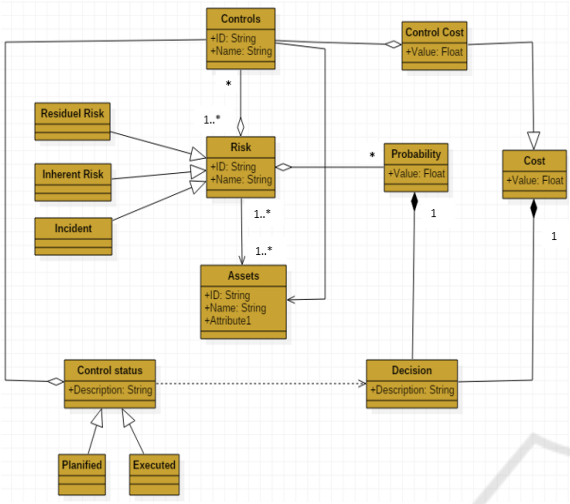

Figure 3: Cost-risk metamodel.

In this conceptual cost-risk model, the inherent risk and the residual risk must be taken into account. The inherent risk is measured by assuming that there is no control or mitigation strategy in place. The residual risk reflects the level of risk following the application of controls and the mitigation of the inherent risks.

Each asset is to be associated with a risk. And depending on the referential, each risk per asset is scored, and a total is computed that represents the global risk of each type of asset. The score of each risk represent the probability that the risk occur.

Control implemented on assets as a mitigation effect the risk and thus reduces its probability to impact the asset. For that, each control has a reduced value of risk. The risks are mitigated by one or multiple security controls. In order to mitigate risk, the total cost of controls to be applied, which is constrained by a maximal available budget, is balanced against the acceptable level of the residual risk (Maximum risk) for each asset.

To summarize, all the components of this conceptual cost-risk model aim to identify the risk mitigation strategies that lead to an optimal trade-off between the costs of the mitigation measures and the achieved risk reduction. This metamodel will be (partially) used to structure the information to be passed from initial reference EAM and risk model to the optimization algorithm.

5 OPTIMIZATION APPROACH

As the number of threats and vulnerabilities continues to grow, a strategy of mitigating all risk equally becomes unsustainable especially when the problem to be solved is complex. First because the risks themselves are not independent (one risk may cause others), and the setting up of controls can itself create new risks. Second, because we must take into consideration the problem of minimizing the cost of controls. However, system administrators are often faced with a more challenging problem since they have to work within a fixed budget that may be less than the minimum cost of controls. The problem is how to select a subset of controls measures so as to be within the budget and yet minimize the residual risk of the system. In this section, we develop an optimisation approach with a Mixed Integer Linear Program (MILP) to solve this problem by formulating a mathematical model derived from the cost–risk model presented previously and then we solve it with Cplex optimizer (ILOG, I., 2012). Cplex is a linear programing solving environment. It is notably based on variant of the Simplex algorithm (Dantzig, G., et al., 1955).

Mathematical Model: Bi-objectives

Here we present the formulated mathematical model used to detail made decisions at the tactical level concerning risk based regulation. This model will decide about the needed mitigation controls that allow to reduce the current risk value to an acceptable level for each asset, and by respecting the budget for risk reduction measures that is limited.

In this section we will define our problem parameters as following:

Definition of Indices:

A: Set of assets a ∈ A
N: Set of Mitigation Controls i ∈ N
M: Set of Risk j ∈ M

Optimization Data Description:

$Caji$ **:** The cost of control i to correct the risk j that impact the asset a
Raj **:** The probability that a risk j impact the asset a
λij **:** The percentage reduction of risk j by the control i
Cost max Raj : The maximal available budget Cost max to correct the risk j that impact the asset a

Risk max j : The maximum acceptable risk value for each asset a

Optimization Constraints Definition

The sum of the costs (Σ C_{aji}) of the mitigation Controls i to be applied to correct each risk j must be less than the maximum budget allocated for each risk impacting the asset a.

$$\sum_{i=1}^{N} Caji \ Xaji \leq Cost \max Raj \quad \forall a \in A, \forall j \in M, \forall i \in N \quad (1)$$

The residual risk should respect the maximum acceptable risk value for each asset a

$$(Raj - (\sum_{i=1}^{N} \lambda ij \ Raj \ Xaji) \leq Risk \max Raj \quad \forall a \in A, \forall j \in M, i \in N \quad (2)$$

The value of risk, control cost and the percentage reduction of risk j by the control i should be greater than zero.

$$Caji, \text{Cost max}, Raj, \text{Risk max}, \lambda ij > 0 \quad (3)$$

Decision Variables

$Xaji =$ 1 If the control i mitigates the risk j that impact the asset a.
0 Else

Objective Function

The objective is twofold: minimize $\sum$ Caji the cost of mitigation controls i of the risks j that impact the asset a and minimize the residual risk value of each risk j .

Minimise

$$\sum_{i=1}^{N} Caji \ Xaji \quad \forall a \in A, \forall j \in M, i \in N$$

Minimise

$$\sum_{i=1}^{N} Raj \ Xaji \quad \forall a \in A, \forall j \in M, i \in N$$

Subject to

$$\sum_{i=1}^{N} Caji \ Xaji \leq Cost \max Raj \quad \forall a \in A, \forall j \in M, \forall i \in N$$

$$(Raj - (\sum_{i=1}^{N} \lambda ij \ Raj \ Xaji) \leq Risk \max Raj \quad \forall a \in A, \forall j \in M, i \in N$$

$$Caji, \text{Cost max}, Raj, \text{Risk max}, \lambda ij > 0$$

6 EXPERIMENTATION AND EVALUATION

In this section we will illustrate on a case study the approach presented above. This case-study is about regulation of risk in a national health-care system. We present the problem of the cost-risk optimization of risk assessment and its mathematical formulation. This optimization approach is included in a broader process involving the several (meta)models presented before

The objective is to study the balance between security risk and cost, and to determine what checks to apply to minimize the value of these two criteria. A resolution of the linear program and an analysis of these results will be evaluated in order to find the optimal solution.

Note that, as our approach could be generalized to type of controls and other kind of threats. Beyond, the present case we can also imagine applied it to any metamodel against the optimization problem.

6.1 Regulation Overview

We here focus on the biomedical analysis laboratory part of the medical domain. We have established an EAM with the participation of key representative partners and with the help of standards (Medical laboratories AT, 2012). The figure 4 summarizes a part of the result of this preliminary work.

We consider a set of 6 assets, in which optimal risk mitigation strategies are identified. The identify-cation of possible strategies and the assessment of the risks and costs associated with these strategies are shown in figure 5. The utilized input data are hypothetical, but they are based on real case studies and they thus reflect an achievable ratio between risk reduction and costs. For all strategies, the net present value of risk and cost are evaluated. These values are presented in figure 5. We aim to select the best strategies that minimize the sum of the net present value of residual risk and costs for each asset.

The Figure 4 and Figure 5 show respectively the relation between Threats and EAM and Control and Threat.

Type	Name	Acts of Human Error or Failure	Software failures or errors	Deviations in quality of service / Compliance challenges	Operational issues	Malware attacks (Malicious software, Ransomware, Spyware and Adware)	Unauthorized use of a health information application
BusinessFunction	BioMedical Analysis	x		x	x		
BusinessfUNCTION	Calibration	x		x	x		
ApplicationComponent	Tracking System		x			x	
ApplicationFunction	Real Time Prescription	x		x	x		
DataObject	Certificates and declarations	x					x
SystemSoftware	IAM - Identity Access Management		x				

Figure 4: Spreadsheet for setting the mappings between EA metamodel and Risk.

	Risk						Control Cost	Reduction
	Acts of Human Error or Failure	Software Failures or errors	Deviations in quality of service / Compliance	Operational issues	Malware attacks (Malicious code, virus, Worm, Trojan	Unauthorized use of a health information system	Value	Value
Security Reminders	X		X	X			25	0,2
Protection from Malicious Software	X			X	X		150	0,28
Log-in Monitoring						X	30	0,1
Password Management	X			X		X	35	0,1
Response and Reporting		X	X				100	0,25
Data Backup Plan							400	0,3
Disaster Recovery Plan		X	X				450	0,5
Emergency Mode Operation Plan				X			200	0,3
Testing and Revision Procedures	X			X			150	0,25
Applications and Data Criticality Analysis							300	0,35
Written Contract or Other Arrangement	X			X		X	65	0,1
Facility Security Plan	X			X		X	150	0,4
Access Control and Validation Procedures				X		X	350	0,3
Maintenance Records		X					125	0,2
probability of risk	18	11	20	18	20	18		
Maximum Acceptable Risk	15	10	15	15	15	5		
Maximal Cost	350	500	900	600	100	800		

Figure 5: Spreadsheet for mappings control on risks.

6.2 Risk Optimization Process

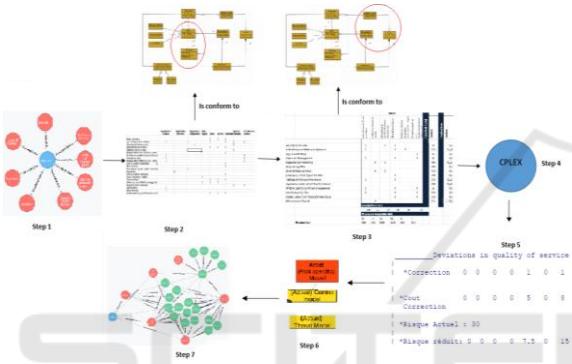

Figure 6: Overall process and involved models.

The first step is the risk optimization process consists in establishing a graph model that identifies the relation between each asset and the different risks. The relation consists in describing which assets a risk potentially impacts. This model is conforms to Archimate metamodel (Lankhorst, Marc M., 2004) to which we added the concept of risk. In the second step, this model is transformed to a model (a table considered as a data model for CPLEX) which represents the mappings between the assets and risks. Also, another data model is established in step 3 to represent the risk mitigations/controls, control cost, the probability that a risk impact an asset, and the reduction value of each control. These values are in this paper manually entered by experts but we can automatize some of those from other data sources (e.g., incident data feed). This two models represented in step 2 and 3 are conform to the metamodel described in figure 3. After that, in step 4, the problematic of cost-risk optimization is described in a mixed integer linear program (described in Section 5) which will be resolved with the IBM ILOG CPLEX optimizer (step5). CPLEX displays the best controls to be applied that allow us to minimize both control costs and the residual risk value. This result can be transformed to a graph model that represents the associations amongst risks, assets and the optimum controls (step7).

6.3 Results

The results of the optimization approach for each asset are summarized in following figures. It shows for each asset the total residual risk $(\mathrm{Raj} - (\sum_{i=1}^{N} \lambda ij \ \mathrm{Raj}\ \mathrm{Xaji}))$.

Figure 7 shows the percentage of risks for each asset. We note that the asset "Real Time Prescription" is the most risky as well as "Biomedical Analysis", while "Identity Access Management" is the least risky with 9% of total risk.

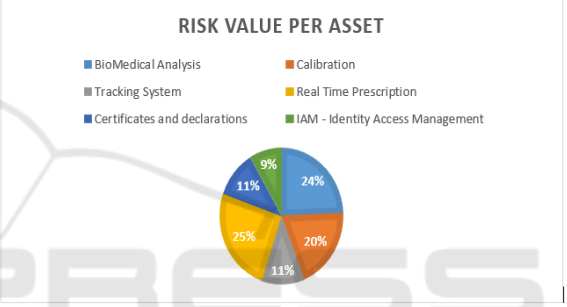

Figure 7: Risk per Asset.

The following figures describe the residual risk after risk mitigation. Here, we explain only the 'BioMedical Analysis' result but the same analysis applies for the rest.

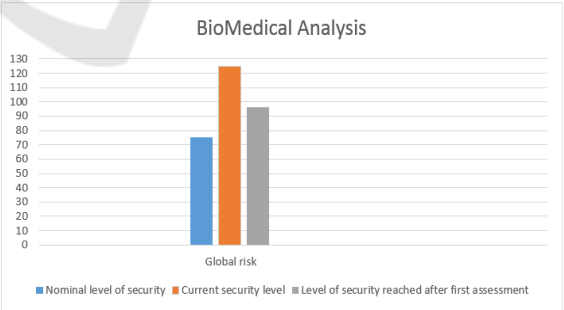

Figure 8: Total residual risk for BioMedical Analysis.

The figure 8 shows a bar chart where the vertical axis of the ordinates bears the risk values.

It has 3 bars that describe three levels of risk: The first stick 'blue' describes the nominal security level (very good). The second stick 'orange' describes the value or safety of current risk (before implementation of controls). The third stick 'grey'

describes the level of security achieved after the implementation of controls (the residual risk).

It is noted that after the first controls, the overall level of risk exceeds the nominal risk level.

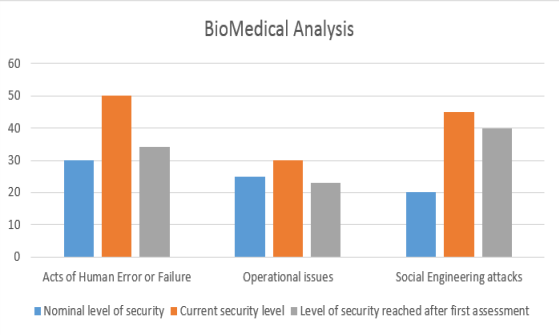

Figure 9: Interpretation risk by risk of Biomedical Analysis.

In the figure 9, we see the risk-by-risk result. It appears that certain risks can be dealt with correctly

This increase in the overall level of risk comes from 'Social Engineering attacks' risk which still exceeds its maximum level for this asset. Moreover, it only decreased by 5%. Whilst the 'Acts of Human Error or failure' risk even exceeds its maximum value, it is at a more or less acceptable level. 'Operational issues' risk is mitigated. It is decreased to an acceptable level.

6.4 Decision Making

There is no optimal solution to achieve the overall level of safety. This result just managed to improve the risk treatment but not to the degree imposed by the risk constraints.

In view of the financial constraints imposed, one can not in any case arrive at the nominal risk, so either the decision maker accepts the risk as it is. It is necessary to alert the Risk Manager about budget constraints and help him to handle the not managed risks.

7 CONCLUSION

In this article we presented a model-driven approach for enterprise-risk management. It is coupled with optimization approach developed through a mixed integer linear program and solved with the optimizer CPLEX. It aims to resolve the problem of selection of optimal risk mitigations controls: it finds the optimal controls that allow minimizing at the same time the residual risk and the cost of controls. It was shown that sometimes the assets cannot be optimized as a whole. We can just manage to improve the risk treatment but not to the degree imposed by the risk constraints and this is due to the financial constraints imposed.

We also show how this optimization phase could be integrated in a more global model-driven approach, all along a given process.

Our future work is to take into account the risk propagation in the graph model obtained at the end of the process and eventually combine it with the optimization process. In that case, a different optimization algorithm, beyond CPLEX, should be implemented. Finally we aim at being more generic against the optimization process and the given metamodels. We aim at providing a facility to describe the elements to optimize on a given metamodel, coupling model-driven approach and optimization.

REFERENCES

Rocchetta, R., Li, Y. F., & Zio, E. (2015). Risk assessment and risk-cost optimization of distributed power generation systems considering extreme weather conditions. *Reliability Engineering & System Safety, 136, 47-61*.

Goettelmann, E., Fdhila, W., & Godart, C. (2013). Partitioning and cloud deployment of composite web services under security constraints. In *Cloud Engineering (IC2E), 2013 IEEE International Conference on (pp. 193-200). IEEE.*

Glover, F. (1997). Tabu search and adaptive memory programming—advances, applications and challenges. In *Interfaces in computer science and operations research (pp. 1-75). Springer US.*

Goettelmann, E., Dahman, K., Gâteau, B., & Godart, C. (2014, June). A formal broker framework for secure and cost-effective business process deployment on multiple clouds. In *Forum at the Conference on Advanced Information Systems Engineering (CAiSE) (pp. 3-19). Springer International Publishing.*

Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing, 9(1), 61-74.*

Xiao, F., & McCalley, J. D. (2007). Risk-based security and economy tradeoff analysis for real-time operation. *IEEE Transactions on Power Systems, 22(4), 2287-2288.*

Dewri, R., Poolsappasit, N., Ray, I., & Whitley, D. (2007, October). Optimal security hardening using multi-objective optimization on attack tree models of networks. In *Proceedings of the 14th ACM conference on Computer and communications security (pp. 204-213). ACM.*

Rodrigues da Silva, Model-driven engineering: A survey

supported by the unified conceptual model Alberto. 2015 The Author. *Published by Elsevier Ltd.*

E. Goettelmann, K. Dahman, B. Gateau, E. Dubois,and C. Godart. A security risk assessment model for business process deployment in the cloud. In Services Computing (SCC), 2014 *IEEE International Conference on, pages 307{314. IEEE, 2014*.

Lankhorst, Marc M. "Enterprise architecture modelling—the issue of integration." *Advanced Engineering Informatics 18, no. 4 (2004): 205-216.*

M. Op't Land, H. A. Proper, M. Waage, J. Cloo, and C. Steghuis. Enterprise Architecture – Creating Value by Informed Governance. *Enterprise Engineering Series. Springer, 2008.*

A. Anaby-Tavor, D. Amid, A. Fisher, A. Bercovici, H. Ossher, M. Callery, M. Desmond, S. Krasikov, and I. Simmonds. Insights into Enterprise Conceptual Modeling. *Data Knowl. Eng., 69(12):1302–1318, 2010.* URL: http://dx.doi.org/10.1016/j.datak.2010.10.003.

El Dabee, F., Marian, R., & Amer, Y. (2014). A simultaneous cost-risk reduction optimisation in JIT systems using genetic algorithms. *IEEE conf. In Control System, Computing and Engineering (ICCSCE).*

Špačková, O., & Straub, D. (2015). Cost-Benefit Analysis for Optimization of Risk Protection Under Budget Constraints. *Risk Analysis, 35(5), 941-959.*

Medical laboratories AT requirements for quality and competence ISO 15189, 2012.

Nicolas Mayer and Jocelyn Aubert. (2014). Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulatio. In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14). ACM, New York, NY, USA, pages 85, 4 pages*.

Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering (pp. 289-306).*

Barbero, M., Jouault, F., & Bézivin, J. (2008, March). Model driven management of complex systems: Implementing the macroscope's vision. In *Engineering of Computer Based Systems, 2008. ECBS 2008. 15th Annual IEEE International Conference and Workshop on the* (pp. 277-286). IEEE.

Salay, R., Mylopoulos, J., & Easterbrook, S. (2009). Using macromodels to manage collections of related models. In *Advanced Information Systems Engineering* (pp. 141-155). *Springer Berlin/Heidelberg.*

Dougherty, B., White, J., & Schmidt, D. C. (2012). Model-driven auto-scaling of green cloud computing infrastructure. *Future Generation Computer Systems*, *28*(2), 371-378.

Deb, K., Pratap, A., Agarwal, S., & Meyarivan, T. A. M. T. (2002). A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE transactions on evolutionary computation*, *6*(2), 182-197.

Sottet, J. S., & Biri, N. (2016). JSMF: a Javascript Flexible Modelling Framework. *FlexMDE@ MoDELS, 2016*, 42-51.

ILOG, I. (2012). CPLEX optimizer. Online. Available: http://www01.ibm.com/software/commerce/optimization/cplex-optimizer.

Dantzig, G., Orden, A., & Wolfe, P. (1955). The generalized simplex method for minimizing a linear form under linear inequality restraints. *Pacific Journal of Mathematics*, *5*(2), 183-195.