Modeling and Simulation of Selected Operational IT Risks in the Banking Sector

Christoph Brandt[1]
Technical University of Berlin, Germany & Public Research Centre Henri Tudor, Luxembourg
email: cbrandt@cs.tu-berlin.de, Christoph.Brandt@tudor.lu

Francesco Santini[2], Natallia Kokash and Farhad Arbab
Centrum Wiskunde & Informatica, Netherlands
email: F.Santini@cwi.nl, Natallia.Kokash@cwi.nl, Farhad.Arbab@cwi.nl

28 September 2012

KEYWORDS

Operational risks, hybrid simulation, control theory, banking sector

ABSTRACT

International banks need to estimate their operational risks due to external regulations. Based on their estimations they need to provide private capital to cover potential losses caused by these risks. Therefore, operational risks need to be properly measured and managed in order to reduce the required private capital. In this paper we discuss operational risks related to a typical banking business process that is enabled by an IT landscape. We present how risks related to the operational behavior of the IT landscape can be simulated. The simulation results help to estimate risk measures like the expected loss, the value-at-risk and the expected shortfall. We further sketch how control theory can be used to actively manage the dynamic reconfiguration of a service landscape, in order to minimize modeled operational risks. First experimental simulation results illustrate our approach.

Introduction

We present a new approach to modeling and simulating operational risks that shows some potential to successfully address open issues known from today's best-practices. The research question is how to model and simulate operational risks of real-world financial organizations using organizational models (Brandt and Hermann (2013)). The main contribution of our work consists of two parts: The first part is about simulating operational risks using an approach that is bottom up and top down at the same time. The second part is about dynamic reconfiguration of service landscapes using control theory, which helps to actively optimize modeled operational risks. The rest of this paper is organized as follows: We, firstly, reflect on the notion of operational risks, introduce a real-world scenario and present the methods and tools that we use. Secondly, we show our first experimental results of an assumed IT landscape as well as a preliminary risk assessment based on these results, and potential next steps of our study. Finally, we discuss selected related work.

Operational Risks

According to the Basel Committee of Banking Supervision *"operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk"* (on Banking Supervision (2011b;a; 2006; 2012)). Operational risks complete the risk portfolio of a bank, which also encompasses credit risks and market risks. Operational risks are largely firm-specific non-systematic risks (Tchernobai (2006)).

In the context of this paper, we focus on the technological risk related to a business process that is enabled by an IT landscape. We measure operational risks by the help of the expected loss, the value-at-risk and the expected shortfall, because these measures nicely integrate with already existing risk frameworks in financial organizations.

A real-world Scenario in Finance Industry

The concrete scenario we consider here was inspired by a study of real-world requirements at Credit Suisse. We decided to go for a business process that is about buying shares over the internet by the help of an e-banking system. In this scenario, people select shares they want to buy, put them into a basket, and finally pay for them using electronic means like credit cards. Once in a while, an account statement is sent to clients by email summarizing all their past transactions.

In order to be able to discuss operational risks related to IT systems, we decided to model a service landscape, which implements and enables this business process. The model is shown in Fig. 1. It comes as a Model-

ica model, running in a Dymola 2013 system. We call this model "Case 1."

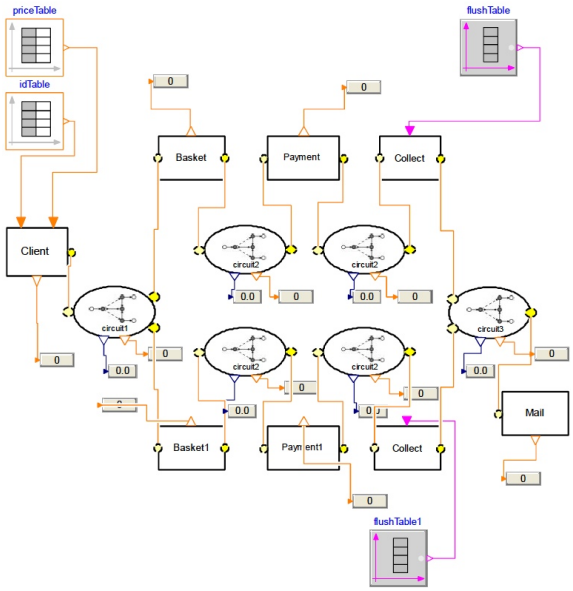

Figure 1: Case 1

In this model, a stream of client orders flows into the system. Each order has a certain business value in euro cents, comes at a specific point in time, and adds up to a concrete basket until that basket is complete.

The input stream in model "Case 1" is replicated (circuit 1) to be processed by an upper (basket, payment, collect) and a lower branch (basket1, payment1, collect1). Because if a request fails in either one of the branches the other one always provides a potential back up. The streams out of the two branches are merged (circuit 3), collected and forwarded from time to time to a mail service, which sends out account statements by email.

The basket services handle the book-keeping of all incoming requests until their corresponding baskets are complete. Once a basket is complete, the whole basket is sent to the payment service. Both services can fail. This behavior is realized by failure distributions. Each of these services has its own failure distribution. The collect services collect all successfully paid baskets and flush them out to the mail service based on a given time table (flushTable, flushTable1). In addition to that, the payment services and the mail services use different delay distributions. The routing between the different services is realized by circuits that internally implement different Reo connectors (Arbab (2004)), which are ideally suited to support the exogenous coordination of services in an IT landscape. These circuits contain buffers, which can run full. In this case, incoming requests are dropped, and, therefore, lost.

Methods and Tools

In this section we introduce the methods and tools that we use and give a short explanation of how we apply them.

Methods: *Reo* (Arbab (2004)) represents a paradigm for composition of distributed software components and services based on the notion of mobile channels. Reo enforces an exogenous channel-based coordination model that defines how designers can build complex coordinators, called connectors, out of simpler ones. Application designers can use Reo as a "glue code" language for compositional construction of connectors that orchestrate the cooperative behavior of instances of components or services in a component-based system or a service-oriented application.[3] Reo supports loose coupling among components and services, distribution of heterogeneous components, exogenous coordination, compositional construction (which nicely matches with the object oriented modeling approach in Modelica), an arbitrary mix of synchrony and asynchrony, user-defined primitives, dynamic reconfiguration, a formal graphical syntax analogous to electronic circuit diagrams, a formal semantics based on coinductive calculus of flow and (alternatively) on constraint automata, and specification and verification methods using programming logic. We use Reo to model the exogenous coordination between the services in our IT landscape. *Hybrid simulations* (Saouma and Sivaselvan (2008)) encompass discrete and continuous simulation techniques at the same time. Discrete simulations are event driven and state based. Continuous simulations represent continuous processes and are usually encoded using differential equation systems. We run hybrid simulations to implement the behavior of constraint automata, which define the semantics of Reo connectors, and we plan to use differential equation systems in order to codify the semantics of control elements. *Control theory* (Bubnicki (2005)) is a theory that deals with influencing the behavior of dynamical systems. The objective of a control theory is to determine corrective actions that lead to system stability. That means, that the system will stabilize at some point and not oscillate. Differential equations describe the input and outputs of a continuous control systems. We rely on control theory to manage the dynamic reconfiguration of Reo circuits.

Tools: Dymola[4] is a simulation engine that supports the simulation of Modelica models. Modelica[5] is a special purpose language for the specification of hybrid simulation systems. Modelica realizes hierarchical model composition, encompasses libraries of truly reusable components and connectors as well as composite non causal connections. Its modeling methodology emphasizes object orientation and equations. Dymola supports graphical composition of Modelica models, and fast simulation with symbolic pre-processing of these models. We use the Dymola/Modelica bundle to model IT landscapes in an object-oriented and graphical way and we use it to run hybrid simulations. Matlab[6] is a numerical computing environment. Its add-on Simulink[7] provides an extensive library of elements for control the-

ory, which are ready to use off the shelf. We use Matlab/Simulink to run control theory models, which actively manage the dynamic reconfiguration of IT landscapes coordinated by Reo circuits in order to optimize operational risks. Matlab/Simulink integrates nicely with Dymola/Modelica as it is possible to run Modelica models, which have been compiled using Dymola, inside a Matlab/Simulink model. Mathematica[8] is a concrete computer algebra system. It comes with an extensive built-in functionality for statistics. We use the symbolic and numerical methods implemented in Mathematica for the risk analysis in our study.

Experimental Results

In this section we present selected experimental results to further illustrate our approach. These results are currently not based on empirical data, but on some random numbers, which we generated based on the insights gained from the analysis of the requirements derived from the real-world scenario at Credit Suisse[9]. The assumptions are strongly simplified in order to comply with disclosure agreements.

We assess the operational risks related to the IT landscape represented by model "Case 1" by simulating its behavior. Therefore, a request stream of incoming orders from different clients is constructed and pumped into the system. We assume that the value of orders is normally distributed, that two to five orders form a basket and that the interval between incoming orders can be represented as a Poisson distribution (Faisst (2003), p.8, Schäl (2003), p.14, Giacometti et al. (year unkown)).

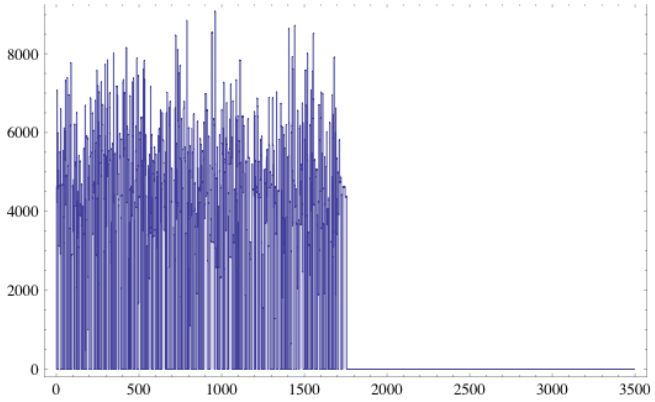

Figure 2: Input Request Stream (x:[s], y:[Euro])

Fig. 2 shows the incoming business value of each request at a certain point in time during the simulation run. Fig. 3 presents the percentage of the most used up first-in-first-out queue in one of the circuits of model "Case 1". The moment one of the queues is full, which means that the used capacity of one of the fifos is at 100% as it can be seen in the figure, the system starts loosing business requests. We analyze these losses from the point of view of operational risks later in this paper. Their accumulated business value in euro cent is shown in Fig. 4.

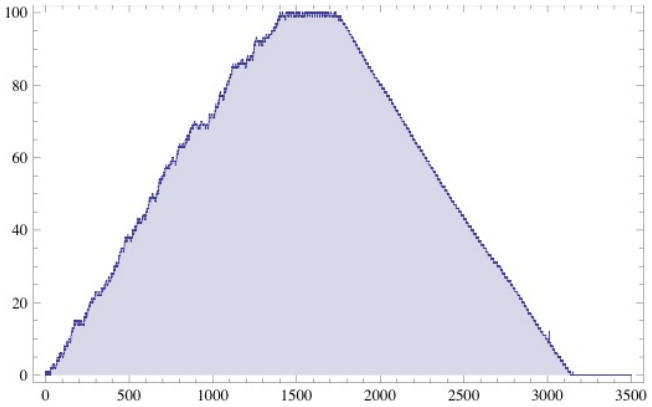

Figure 3: Used FIFO Capacity (x:[s], y:[%])

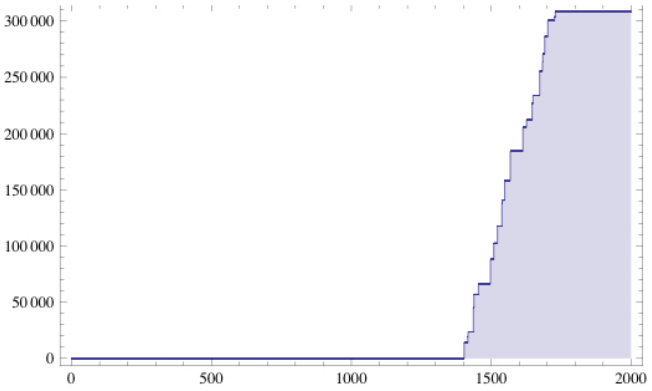

Figure 4: Accumulated FIFO Losses (x:[s], y:[Euro])

In our system, losses do not occur only due to full queues, but also because services fail to operate successfully. This failure can have internal or external reasons. An internal reason may be that a service is defective, an external reason may be that some needed external services do not provide expected results. In the scope of our study we realized service failures as simple failure probabilities. Fig. 5 shows the accumulated business value that was lost during the simulation run due to failures of different services in model "Case 1." As it can be seen, service failures happen from the very beginning, whereas fifo losses start happening once one of the queues is full.

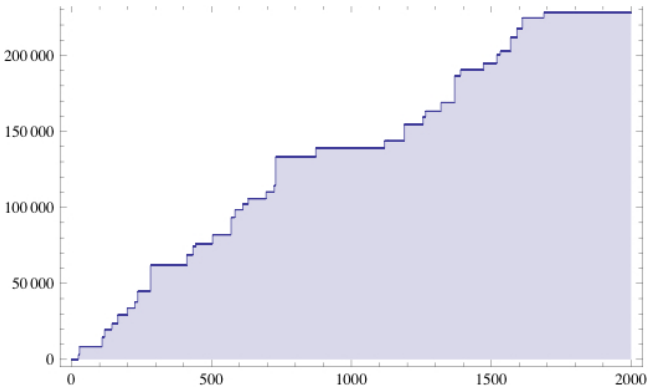

Figure 5: Accumulated Service Losses (x:[s], y:[Euro])

We will see in the following that these different types of losses result in different shapes of loss distributions that are counterintuitive, and which contradict today's assumptions about the shape of loss distributions of operational risks.

In our model "Case 1" paid baskets are collected in the collect services. Afterwards, account statements are sent out on a regular basis using a time table. Fig. 6 shows the total business value related to these account statements that are sent out at certain points in time.

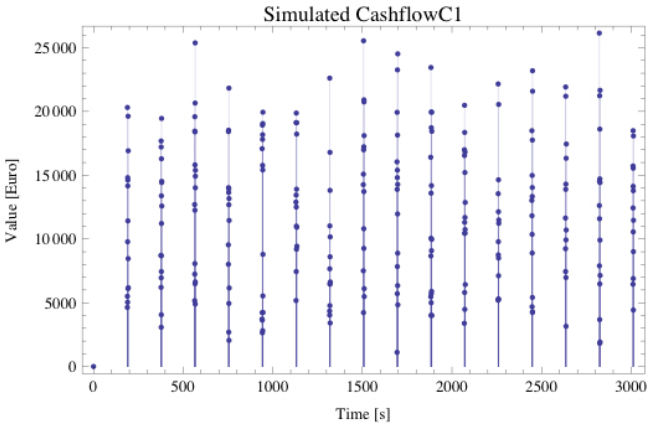

Figure 6: Simulated Cash Flow (x:[s], y:[Euro])

We defined the accumulated business value as the obtained cash flow of successfully executed business processes.

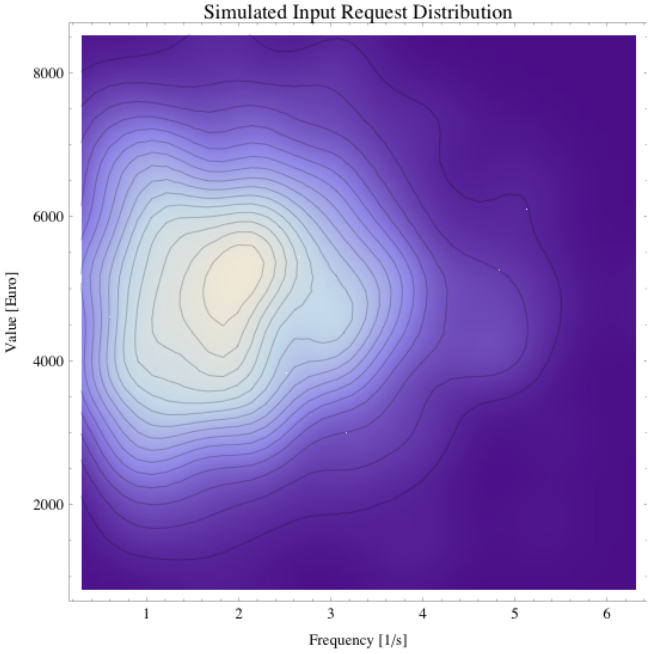

Figure 7: Simulated Input Requests (x:[1/s], y:[Euro])

In line with today's practice for operational risks we present our finding using value and frequency distributions. In Fig. 7 the copula of the value/frequency distribution of the input requests is presented, which are based on generated random numbers. Here, this copula looks as if it is built out of two independent distributions, which is, in fact, in line with the setting of our simulation run, and, therefore, not surprising, the outcoming results correspond to the inserted variables. Assuming now independent value and frequency distributions, estimating their parameters and constructing a copula leads to the result presented in Fig. 8. In the given case, we used a normal distribution to approximate the simulated value distribution and a Poisson distribution to approximate the simulated frequency distribution. Both theoretical distributions fit the simulated distributions.

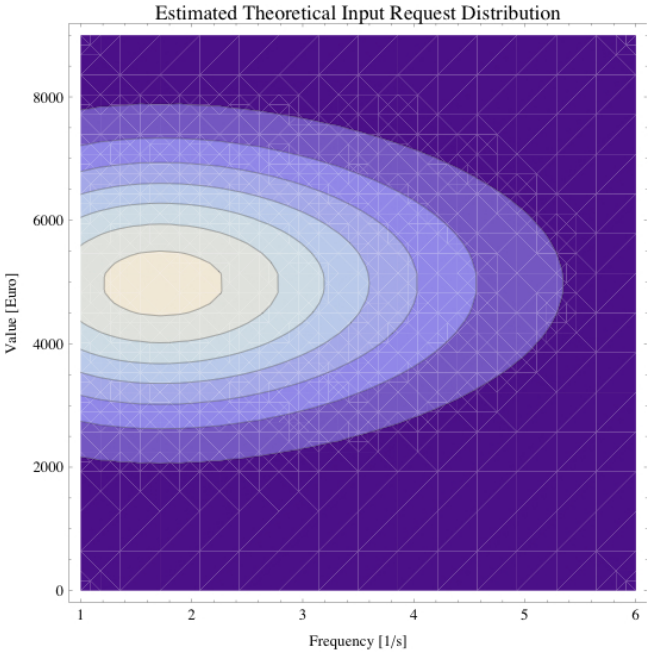

Figure 8: Estimated Input Requests (x:[1/s], y:[Euro])

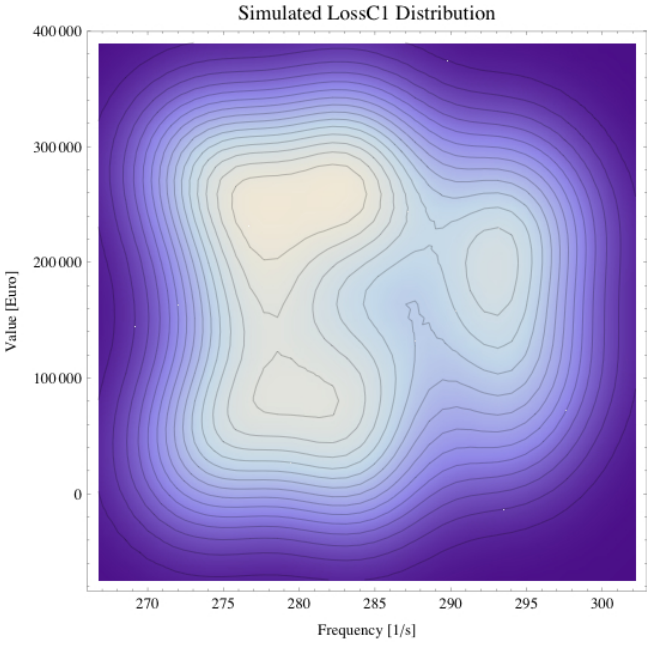

Figure 9: Simulated FIFO Losses (x:[1/s], y:[Euro])

We see a completely different situation in Fig. 9. Here,

the copula of simulated losses due to full queues is shown. The picture indicates that the underlying frequency and value distributions are not independent.

We can see two centers of high value and low value losses at a low frequency and one center of high value losses at a high frequency. This experimental result supports the statement made in Tchernobai (2006) that *"unlike market risk and perhaps credit risk, the [operational] risk factors are largely internal to the bank."* What we see is the structural impact a concrete IT landscape has regarding the observable loss behavior.

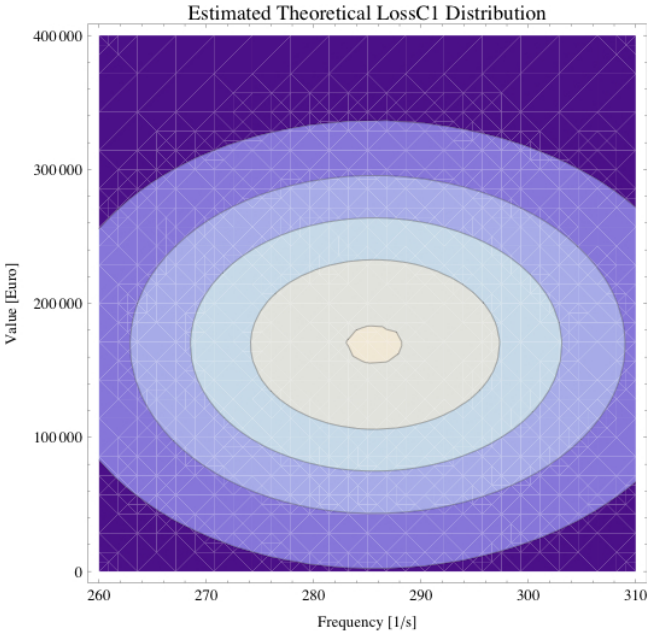

Figure 10: Estimated FIFO Losses (x:[1/s], y:[Euro])

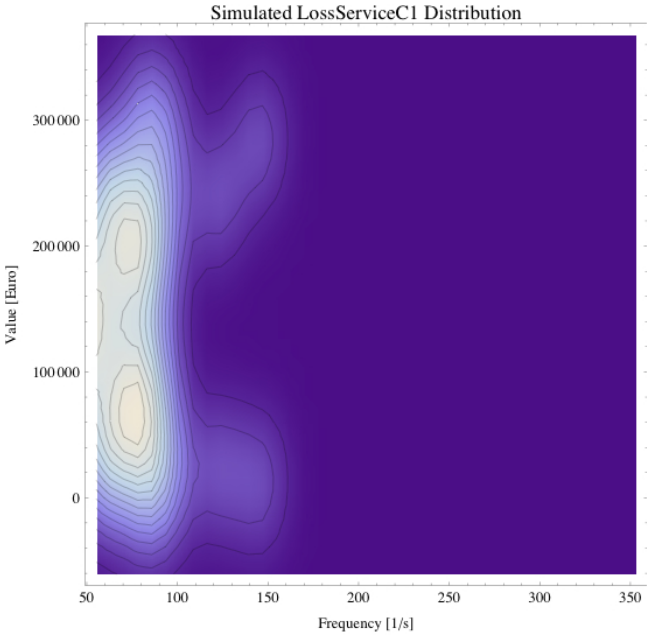

Figure 11: Simulated Service Losses (x:[1/s], y:[Euro])

In Fig. 10 we present the estimated copula based on the obtained simulation data. It is based on the assumptions of independent value and frequency distributions. As suggested in (Tchernobai (2006)) the value distribution is approximated using an alpha-stable distribution, the frequency distribution is built up using a Poisson distribution. However, as can be seen, the assumptions do not hold. The shape of the estimated copula is significantly different from the shape of the simulated copula. This shape mismatch indicates that top down measurement approaches do not always work well. A much better match between the simulated and the estimated loss distributions related to service failures can be seen in the following. In Fig. 11 the simulated service losses are shown.

In Fig. 12 the estimated theoretical copula is presented based on the same assumptions as before, in Fig. 10. The potential reason for this match is that the overall structure of the IT landscape has much less influence on independent loss events in different services than routing decisions of requests have when losses in queues are analyzed.

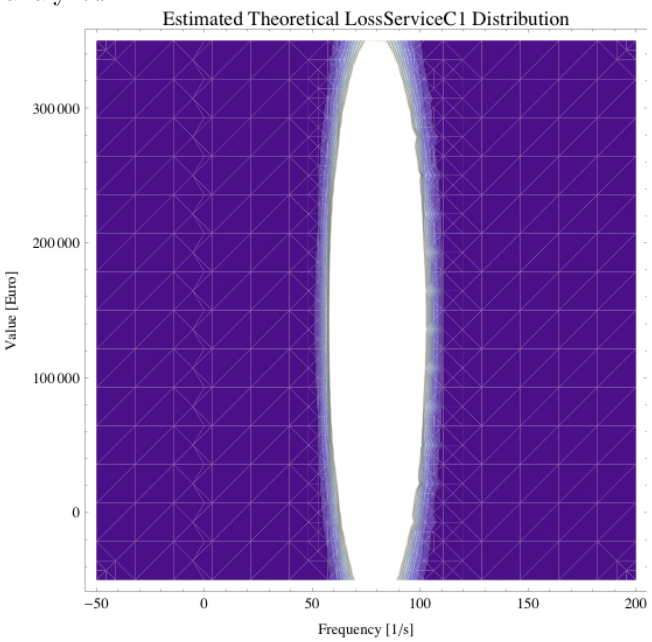

Figure 12: Estimated Service Losses (x:[1/s], y:[Euro])

However, what we can see is that the value of baskets is no longer normally distributed. There are two centers visible in Fig. 11, and there are apparently two different loss distributions operating, one that causes many losses, and one that cause only few losses. This observation is in line with the settings of our simulation model, the outcoming results correspond to the inserted variables. However, our settings should make sense because, in practice, the individual loss behavior of a specific service application should be specific to that service or application.

Fig. 13 finally shows the simulated copula of the successfully obtained cash flow in the end. We can see four centers. A low frequency/low value, a low frequency/high value, a high frequency/high value and a

high frequency/low value centers.

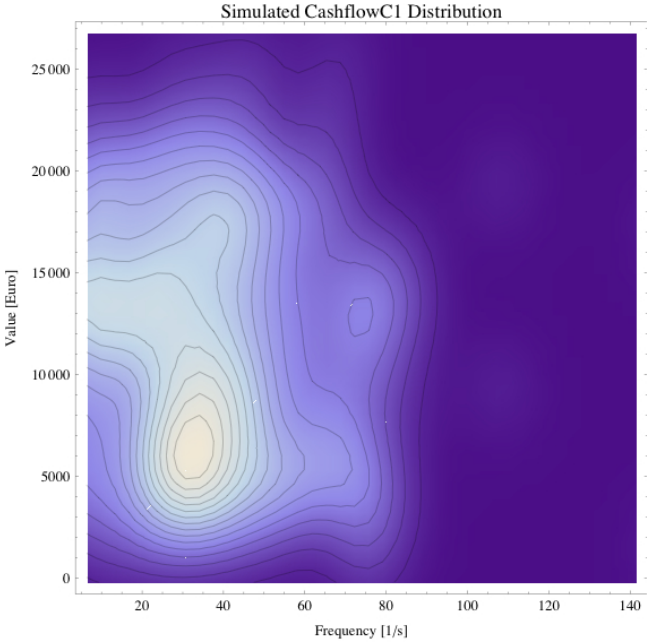

Figure 13: Simulated Cash Flow (x:[1/s], y:[Euro])

As in previous cases, this phenomenon is caused by the specific qualities of the IT landscape in model "Case 1." Here, again, the estimated theoretical copula, in Fig. 14, oversimplifies the situation. Therefore, the often advertised top down approach recommended to estimate distributions for operational risks does not successfully work here.

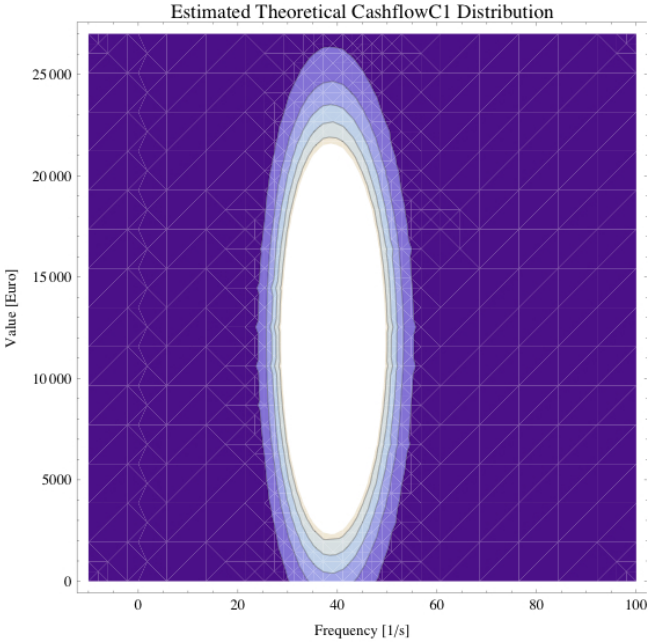

Figure 14: Estimated Cash Flow (x:[1/s], y:[Euro])

Experimental Risk Assessment

In the literature (Tchernobai (2006), Daldrup (2005)) the loss distribution is used to estimate the expected loss, the value-at-risk and the expected shortfall. Whereas the expected loss can be priced into the products and services, the value-at-risk is used to determine the needed capital to cover potential, but unforeseen losses. In addition to that, the expected shortfall can be used to optimize a portfolio of operational risks. In the following, we suggest doing this using control theory, whereby a controller governs the automatic re-configuration of Reo circuits that exogenously coordinates services in our assumed IT landscape.

In Fig. 15 an alpha-stable distribution is shown describing the loss behavior of the simulated system. Its parameters have been estimated using bootstrap techniques applied to the simulated data. To take an alpha-stable distribution in order to model operational risks was suggested by (Tchernobai (2006)). Here, the distribution fits the data generated by the simulation and was accepted by all goodness-of-fit tests we checked. From left to right vertical lines represent the expected loss, the value-at-risk and the expected shortfall for the simulated period and for a confidence level of 0.95 on a per business request basis. According to Tchernobai (Tchernobai (2006)) different confidence levels lead to different capital requirements. In order to keep our underlying (numerical) simulation issues simple, we decided to calculate the risk measures for the purpose of demonstration in the scope of this paper for a confidence level of 0.95. However, current regulations (on Banking Supervision (2006) p. 151) require a confidence level of 0.99 or 0.999.

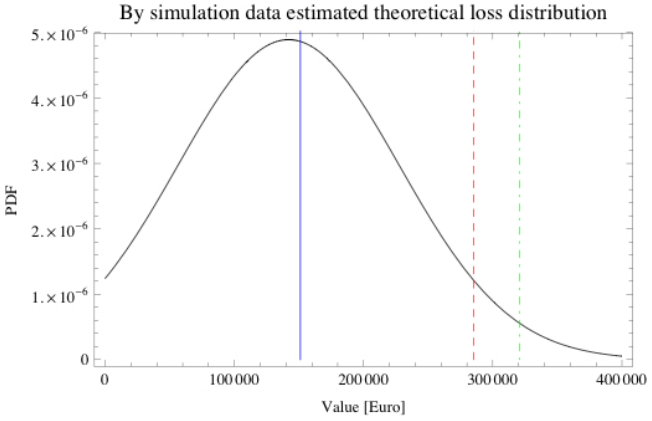

Figure 15: Risk Measurements for Losses (x:[Euro], y:[PDF])

In principle, the same can be done for the cash flow in a symmetric way. The theoretical distributions here are still under investigation and left for future work.

However, the loss distribution covers all losses that occur during the simulation, that is, losses of services and losses because of full queues. As we have seen in earlier figures, some loss distributions are impacted by the structural qualities of the simulated system, whereas others are not. Therefore, the fit of the alpha-stable distribution describing the loss behavior of a system in the given case cannot yet be generalized as it was sug-

gested in Tchernobai (2006).

Therefore, the approach we apply is at the same time bottom up and top down. It is bottom up as it generates simulation data of the potential future behavior of a system, which can be used in exchange of past loss data. It is top down as it estimates parameters of theoretical distributions based on the generated simulation data, which are selected based on a priori assumptions. The advantage is clear. Past data do not necessarily reflect the future loss behavior of a system because IT landscapes constantly change. Simulation provides a look-ahead, which fixes this problem. Secondly, today's approaches to estimating operational risks are built on top of data pools. These pools no longer reflect structural information needed to assess operational risks. Here, simulation can help as it is not (necessarily) built up on whole organizations, but on organizational elements, which may appear in different contexts and are more stable than organizations as such. Therefore, we suggest to focus on organizational building blocks, setting them up each to represent a concrete organizational setting, and simulating them in order to derive the necessary data for risk assessment.

Next Steps

The next steps in our study will focusses on the simulation of the model "Case 2". Here, we assume that incoming orders are not replicated and simultaneously processed by an upper and a lower branch, but arbitrarily distributed to the available services in order to maximize the overall capacity of requests the IT landscape can process. Fig. 16 shows the Modelica model of "Case 2" in the Dymola environment.

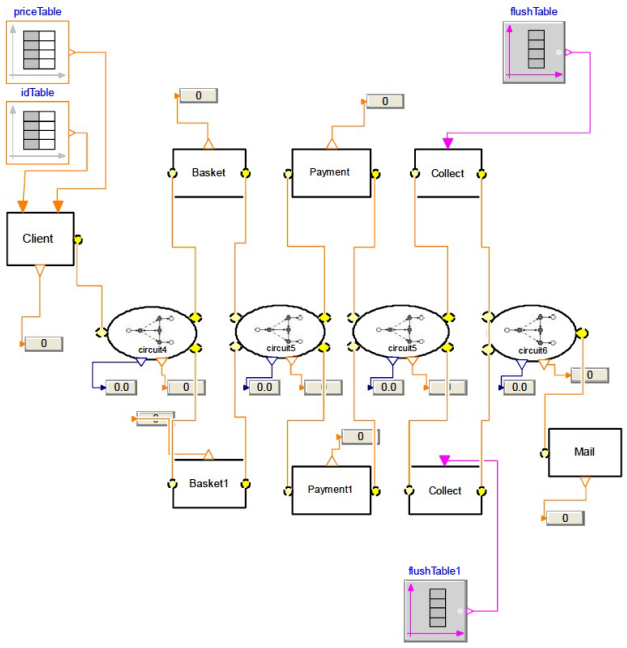

Figure 16: Case 2

The main differences compared to model "Case 1" in Fig. 1 are the different Reo circuits that coordinate the used services.

Our assumption is that model "Case 1" is better in terms of operational risks when few requests of high value need to be processed, whereas model "Case 2" excels when many requests of low value need to be handled. The corresponding simulations are left for future work.

Assuming that the nature of the incoming requests may change over time, as for instance, typical business situations at day and at night differ, model "Case 3" in Fig. 17 combines both earlier models. It contains a switch that either selects model "Case 1" or model "Case 2" for processing the incoming requests. From a theoretical point of view, the switch enables the dynamic reconfiguration of the Reo circuits in the given IT landscape by either selecting the first or the second configuration. We plan to control the switch by setting variables of the switch to certain values through a control model. We assume that the control model can at the same time read certain variables indicating the situation of operational risks from model "Case 1" and model "Case 2", respectively.

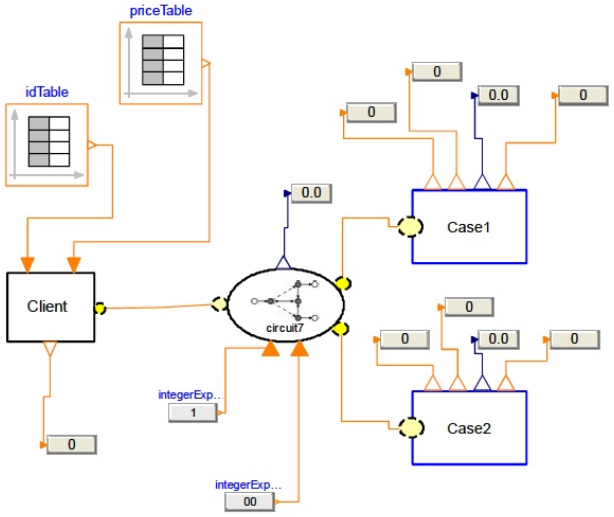

Figure 17: Case 3

Subsequently, we wrapped model "Case 3" in the Matlab/Simulink environment and defined input and output ports declared in the Dymola/Modelica setting. This enables us to use "Case 3" as a black-box in this environment. Currently, this Matlab/Simulink model just reads generated random data created using Mathematica and writes simulation data into result files. In the future we plan to use the Matlab/Simulink libraries to develop the control model which then either decides to switch to the first or the second Reo configuration. To the best of our knowledge our suggested approach of using a control model in order to switch between Reo configurations of a service landscape in order to optimize the modeled operational risks is new and has not been

published thus far. It requires further investigation to determine how to best capture the real operational risks by the help of the modeled operational risks in order to finally optimize the real operational risks.
Fig. 18 presents the general nature of a control model. The target system represents model "Case 3." So, the control model still needs to provide the controller and the transducer. The target system can be disturbed by external noise or stochastic input data. The transducer transforms the measured output from the target system into a transduced output, which is compared with a reference value that can stand for an accepted level of operational risks. The delta or control error is then used by the controller to provide the necessary control input for the target system in order to reduce the control error.

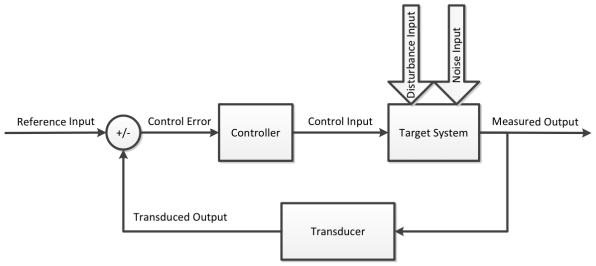

Figure 18: Feedback System

Related Work in Operational Risk Analysis

Three PhD theses have served as a constant source of inspiration during our work on operational risks. The first one is by Anna S. Tchernobai (Tchernobai (2006)). It presents contributions to modeling of operational risks in banks and comes up with an exceptional in-depth statistical treatment of available loss data. The second one is by Anja Hechenblaikner (Hechenblaikner and zu Selhausen (2006)). It presents contributions related to operational risks in banks and provides an outstanding methodological analysis of how to measure operational risks from qualitative and quantitative points of view. The third one is by Britta Kunze who did an outstanding job of analyzing the regulatory sources of operational risks (Kunze and Poddig (2007)). Finally, in his excellent paper, Andre Daldrup (Daldrup (2005)), discusses with impressive clarity different approaches to risk measurement, their strengths, weaknesses and potential uses.

Related Work in Enterprise Architectures

A discussion about the regulatory perspective in enterprise architectures can be found in van Bommel et al. (2007). Here, the question of implementing regulatory requirements into an enterprise architecture or enforcing them using flexible business rules shows up. By anchoring regulatory requirements into an assumed control model we serve both views. The control model is an architectural choice, its parameterization, however, provides room for flexibility in the sense of dynamic business rules.
From the point of view of setting up an Information System Security Risk Management (ISSRM) system, Nicolas Mayer provided a reconstructed domain meta-model that helps to capture all potential risks covered by current industrial standards Nurcan et al. (2010), Mayer (2009). In contrast to that, we covered just selected risks in an assumed IT landscape in order to demonstrate the potential advantages of our simulation approach.

Results and Future Work

Reviewing our main research questions, we were able to provide contributions in the following areas: First, we present an approach to simulating operational risks using hybrid simulation techniques. Our simulated data enabled us to look ahead instead of looking back. Further, the simulation preserved the structural information of the system in the simulated distributions. The simulated data can be used to estimate parameters of given theoretical distributions. Second, we combine control models with Reo models to enact dynamic reconfiguration of service landscapes with the aim to minimize the overall operational risks over time in an actively managed way.
Potential future work entails extending the given scenario by external service providers that offer additional capacity to the system landscape. In this context, market prices for services show up. The handling of shared resources like services that run on shared servers, needs to be studied and the competitiveness of "Case 3" in combination with a control model needs to be validated versus "Case 1" and "Case 2". Likewise, the effectiveness and efficiency of our approach must be compared with today's best practices. In addition to that, it appears useful to check if the presented approach is appropriate to fulfill the AMA criteria, and to check which impulses for the daily business of a bank could be generated using it. It may also be interesting to look deeper into the question of what has to be done in order to integrate our approach in the risk bearing ability in Pillar II of Basel 2, and to think about using the results to support the construction of computational methods, as well as the design of non-deceivable risk regulations, that can be applied by regulation authorities.

Acknowledgements

We like to thank the anonymous reviewers for their helpful comments and Prof Dr Thomas Engel of the SnT at the University of Luxembourg (`http://wwwen.uni.lu/snt`) for his feedback about the obtained results, especially for the discussion of potential follow-up research questions about the design of future regulations.

Notes

[1]This work has been partially sponsored by the *Fonds National de la Recherche Luxembourg* (www.fnr.lu), via the PEARL programme.

[2]This work was carried out during the tenure of the ERCIM "Alain Bensoussan" Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission.

[3]http://www.reo.project.cwi.nl

[4]http://www.3ds.com/products/catia/portfolio/dymola

[5]http://modelica.org/

[6]http://www.mathworks.nl/products/matlab/

[7]http://www.mathworks.nl/products/simulink/

[8]http://www.wolfram.com/mathematica/

[9]Credit Suisse (Luxembourg) S.A., P.O.BOX 40, 56, Grand-Rue, L-2010 Luxembourg.

REFERENCES

Arbab F., 2004. *Reo: a channel-based coordination model for component composition. Mathematical Structures in Computer Science*, 14, no. 3, 329–366.

Brandt C. and Hermann F., 2013. *Conformance Analysis of Organizational Models in a new Enterprise Modeling Framework using Algebraic Graph Transformation. International Journal of Information System Modeling and Design (IJISMD)*, 4, no. 1.

Bubnicki Z., 2005. *Modern control theory*. Springer. ISBN 9783540239512.

Daldrup A., 2005. *Kreditrisikomasse im Vergleich. Universität Göttingen, Wirtschaftsinformatik II - Arbeitsbericht*, , no. 13, 1–33. http://www2.as.wiwi.uni-goettingen.de/getfile?DateiID=571.

Faisst U., 2003. *Ein Modell zur Steuerung operationeller Risiken in IT-unterstutzten Bankprozessen*. In *Multikonferenz Wirtschaftsinformatik 2004, Diskussionspapier WI-138*. 1–19. http://www.wi-if.de/paperliste/paper/wi-138.pdf.

Giacometti R.; Rachev S.; Chernobai A.; Bertocchi M.; and Consigli G., year unkown. *Practical Operational Risk*. http://statistik.ets.kit.edu/download/doc_secure1/JOR-Practical-Operational-Risk-GRCBC.pdf.

Hechenblaikner A. and zu Selhausen P., 2006. *Operational Risk in Banken: Eine Methodenkritische Analyse Der Messung Von It-Risiken*. Bank- Und Finanzwirtschaft. Deutscher Universitätsverlag. ISBN 9783835004245.

Kunze B. and Poddig P., 2007. *Überwachung operationeller Risiken bei Banken: Interne und externe Akteure im Rahmen qualitativer und quantitativer Überwachung*. Gabler Edition Wissenschaft. Deutscher Universitätsverlag. ISBN 9783835006430.

Mayer N., 2009. *Model-based Management of Information System Security Risk*. Ph.D. thesis, University of Namur. http://www.nmayer.eu/publis/Thesis_Mayer_2.0.pdf.

Nurcan S.; Salinesi C.; Souveyet C.; and Ralyté J., 2010. *Intentional Perspectives on Information Systems Engineering*. Springer. ISBN 9783642125430. URL http://books.google.lu/books?id=4rc4_3gJPOIC.

on Banking Supervision B.C., 2006. *International Convergence of Capital Measurement and Capital Standards*. Bank for International Settlements. http://www.bis.org/publ/bcbs128.pdf.

on Banking Supervision B.C., 2011a. *Operational Risk - Supervisory Guidelines for the Advanced Measurement Approaches*. Bank for International Settlements. ISBN 9789291318568. http://www.bis.org/publ/bcbs196.pdf.

on Banking Supervision B.C., 2011b. *Principles for the Sound Management of Operational Risk*. Bank for International Settlements. ISBN 9789291318575. http://www.bis.org/publ/bcbs195.pdf.

on Banking Supervision B.C., 2012. *Consultative Document - Principles for effective risk data aggregation and risk reporting*. Bank for International Settlements. http://www.bis.org/publ/blbs222.pdf.

Saouma V. and Sivaselvan V., 2008. *Hybrid Simulation: Theory, Implementation and Applications*. Balkema-proceedings and monographs in engineering, water, and earth sciences. Taylor & Francis. ISBN 9780415465687.

Schäl I., 2003. *Die Quantifizierung und Steuerung von operationellen Risiken*. zeb. http://www4.wiwi.uni-karlsruhe.de/MITARBEITER/SCHAEL/OperationelleRisiken.pdf.

Tchernobai A.S., 2006. *Contributions to Modeling of Operational Risks in Banks*. PhD Thesis. University of California Santa Barbara. http://gradworks.umi.com/32/18/3218836.html.

van Bommel P.; Buitenhuis P.; Hoppenbrouwers S.; and Proper E., 2007. *Architecture Principles - A Regulative Perspective on Enterprise Architecture*. In M. Reichert; S. Strecker; and K. Turowski (Eds.), *EMISA*. GI, *LNI*, vol. P-119. ISBN 978-3-88579-213-0, 47–60.