A Comprehensive Approach to Assess Operational Resilience

R.J.M.Stolker [1], D.M.Karydas [2], and J.L. Rouvroye [3]
Eindhoven University of Technology, Den Dolech 2, P.O. Box 513, 5600 MB
Eindhoven, the Netherlands
[1]R.J.M.Stolker@student.tue.nl
[2]D.M.Karydas@tue.nl
[3]J.L.Rouvroye@tue.nl

Abstract. This paper presents a first attempt to apply Multi-Attribute Utility Theory (MAUT) to the concept of resilience. The focus of this paper is measuring the management performance of *operational resilience* in an organization. Operational resilience refers to the ability of an organization to prevent disruptions from occurring as well as the ability to respond quickly to and recover from a disruption in the primary business processes. A value tree is constructed containing the attributes that contribute to resilience management. Elements included are among others: understanding mission-critical processes, risk management performance, reward system, and cultural aspects. A checklist is used to measure how an organization performs on the attributes of resilience. This provides an approach to measure operational resilience. The checklist has been validated by auditing three organizations and through the use of case studies derived from the work of Sheffi (2005).

1 INTRODUCTION

According to Klein et al. (2003) resilience can be traced back to the Latin word *resilire* which means "to jump back". The general character of the word resilience has led to a wide application of the concept; it can be found in many disciplines, such as engineering/safety systems, ecology, risk management, psychology, and sociology (Fiksel, 2006). Among the different disciplines, the focus here is a risk-based approach of resilience. More specifically, risks related to operational processes in organizations.

1.1 The Nokia-Ericsson Case: Operational Resilience

Before discussing operational resilience, an illustrative example described in more detail by Sheffi (2005) is given. It shows a resilient company and a less resilient company. The companies involved are Philips NV, the Dutch electronics company with an industrial facility in Albuquerque, and Nokia and Ericsson, both regular customers of Philips, both purchasing chips used for their cell phones. On Friday night, March 17, 2000, lightning

struck a Philips industrial building starting a fire. Philips announced an expected one-week delay to Nokia and Ericsson. Interestingly, the companies responded differently to this announcement. Nokia responded by internalizing the bad news and identified which chips came from that plant. Moreover, a troubleshooter was informed who started working on the issue. Ericsson assumed that the chips would be delivered with some delay. It even got worse, because after further investigation Philips announced that it would take weeks to restart the production and might take months to catch up on the production schedule. Nokia quickly assembled a team of 30 officials from around the world to find a solution for this major problem. Nokia found other suppliers for three of the five types of chips, but two types only came from Philips. The Nokia team insisted on rerouting the capacity of Philips. By the time Ericsson realized the magnitude of the problem, it was too late. Philips could not help anymore because Nokia had already claimed the spare capacity. Unlike Nokia, Ericsson did not have alternative suppliers available to produce the chips. As Ericsson's marketing director for consumer goods said: "We did not have a plan B". The consequences were therefore different for the companies; within six months of the fire Nokia's share of handset market increased from 27 to 30 percent, while Ericsson's dropped from 12 to 9 percent.

This example illustrates the context of this research, namely risks related to operational processes. Both Nokia and Ericsson produce cell phones and this process was disrupted due to delayed supply of components (chips). The operational process refers to the input – transformation – output process and related support processes (e.g. ICT) of a company. Additionally, this example also illustrates which company is better able to respond to disruptions and which lessons can be learnt to become resilient.

1.2 Definition of Operational Resilience

The perspective used to describe the operational process of an organization is the commonly used systems approach, and more specifically that of complex adaptive systems (McManus et al., 2007). In general, one can state that organizations are complex adaptive systems because they consist of many interrelated entities and are able to change and learn (implying they are adaptive). In this context, the description for resilience given by McDonald (2006) seems most appropriate: "resilience probably needs to be seen as an aspect of the relationship between a particular socio-technical system and the environment of that system". The environment is potentially very broad, including external social and commercial factors. However, the focus of this research is on operational risks while strategic, market, financial, and legal risks are beyond the scope of this research. For this reason, the term operational resilience is introduced here. The capabilities of an organization related to operational resilience are:

- The ability of an organization to *prevent* disruptions from occurring;
- When struck by a disruption, the ability to quickly *respond to* and *recover from* a disruption in the primary business processes.

Operational resilience is about the ability of an organization to deal with undesired events. These events can have a high or low impact and they can have a high or low probability of occurrence. Resilience is most applicable to low-probability/high-impact

events as the other combinations should have been covered either up-front (high-probability/high-impact) or during normal operations (high-probability/low-impact) or neglected (low-probability/low-impact). This is one of the reasons that the concept of resilience has been introduced, namely as a capability to deal with low-probability/high-impact events (Sheffi, 2005).

There are three main reasons that stress the need for resilient organizations. First of all, for organizations it is of utmost importance that they are able to respond quickly to low-probability/high-impact disruptions in order to minimize cost and damage. The consequences can be severe if a company is not able to deal with these disruptions: financial and human losses, critical damage to image, lost market share and the like, as illustrated by many case studies in Sheffi (2005). Secondly, companies are faced with increased vulnerability because they are subject to more and unforeseeable risks. For example, globally distributed supply chains make companies makes companies more dependent on each other. Finally, despite the importance, the lack of business continuity plans in today's companies indicates that companies are not well prepared for disruptive events (Callagher, 2003; Chapman, 2006).

1.3   Measurement of Operational Resilience

The interesting issue about resilience is about what makes companies resilient and how companies can measure their resilience. If a company should be resilient, the company must know how it can become resilient, and how it can improve if it lacks resilience in the current situation. Several attempts have been made to address the issue of measuring (characteristics of) resilience. For example, assessing the continuity of business processes by the British Standard Institute (BSI, 2007) resulted in BS25999. Another element of resilience is measuring the safety culture in an organization as suggested by Flin (2006). However, no comprehensive approach for assessing resilience is currently available that covers the different elements of resilience as described by various researchers. This is the basis for the research question: *How can operational resilience be assessed in a comprehensive manner?*

This research attempts to develop a generic approach to measure operational resilience. Based on this approach a company will receive an indication of its resilience and indications of potential improvements so that it is better able to deal effectively with risks and disruptive events in this more turbulent world. The intention of this research is to develop an approach that assesses an organization's resilience very fast, approximately in a few hours. A precondition is that the organizational member(s) involved have preliminary knowledge of the risk management practices within the organization as well as of the approaches being used.

2   HIERARCHICAL METHOD TO MEASURE RESILIENCE

The multi-attribute utility theory (MAUT) is used to measure resilience. The first reason of using MAUT is to deal with complexity because resilience has many different meanings and characteristics. A method within MAUT called the value tree enables to decompose a complex objective (here: operational resilience) into attributes. An attribute

measures performance in relation to an objective. These attributes are called Performance Measures (PM). In this way, resilience can be measured. A second reason is that it allows prioritization by assigning weights to attributes and objectives. This weighing is performed by the stakeholders based on what they consider important to resilience. Prioritization in turn supports decision making to tackle resilience problems in companies. For example, resource allocation in companies can be based on priorities of attributes that contribute most to resilience. Though the actual prioritization was not part of this research, this second advantage was an additional reason to construct a value tree (see Figure 1). The weighing of attributes and objectives differs for each company based on the stakeholder's preferences. Although even the value tree can differ in a company, the value tree presented in this paper may be used in other companies or used as a steppingstone.

2.1 Resilience Management Performance

A literature search resulted in many but still not directly measurable characteristics, such as top-level commitment, culture, awareness, flexibility, security, redundancy, and (crisis) communication. All these characteristics contribute (in)directly to a company's resilience capabilities. These are potential attributes in a value tree. However, there are requirements that must be met according to MAUT. The most important one is additive independence among the PMs (Apostolakis & Lemon, 2005). This means that there cannot be dependencies among the PMs because then elements may be measured twice. This is a strong requirement but can be assumed in some circumstances. Since this research is a first attempt to decompose and measure resilience, the aim is to obtain an indication of operational resilience. Similar to Apostolakis & Lemon (2005), additive independence is a reasonable assumption to make in this case, because the results are treated as a "useful first-cut approximation" (Clemen, 1991).

As said, after identification of characteristics there were difficulties in making them measurable. Constructing a value tree is an iterative bottom-up / top-down process, but the bottom-up approach was used here. This approach is recommended by Forman & Selly (2001) in situations with uncertainty. Thus, first the PMs were constructed rather than the objectives. Since many different strategies can be pursued by companies to deal with operational risks and since this research aims at developing an approach applicable to every organization, the focus will be on how companies have *managed* these risks. Accordingly, this approach measures an organization's *resilience management performance*. In other words, are there any management practices in the organization that contribute to continued operations and how thorough are these practices performed? Literature from business continuity management, Health, Safety, and Environment (HSE), and resilience management have been consulted to develop checklists for specific elements of resilience. The bottom-up approach enabled to check whether all elements of the various sources were included in PMs. This ensures another requirement of the value tree: completeness. These checklists can be used as PMs for attributes of resilience. A classification of objectives and attributes has been made based on these checklists. The resulting value tree is shown in Figure 1.
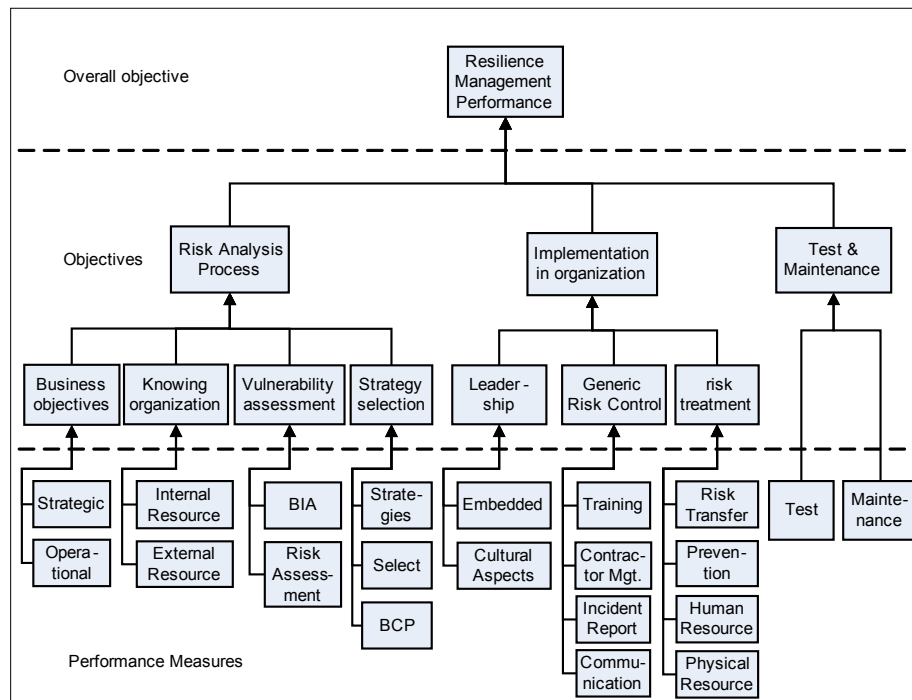
Fig. 1. The value tree of operational *resilience management performance*. Overall objective is to obtain a score of the company's resilience management performance. The scores obtained from all the *Performance Measures* at the bottom of the value tree and the weights assigned to attributes and *objectives* determine the overall score of resilience

Each lowest-level objective can be measured by one or more PMs. In total there are 21 PMs that measure the eight higher-level objectives. An example of a PM is given for the objective '*Generic Risk Control*' in Table 1. It shows the checklist related to PM 6.2 and measures how well a company has performed *Contractor Management*. In total, there are three more PMs assessing how well a company has implemented generic risk control measures, namely '6.1 Training', '6.3 Incident Report', and '6.4 Communication'. The reader may refer to the complete research that will be published on www.tue.nl/bib.

The score that can be obtained for resilience management performance differs for each company. This depends on the assignment of weights to the attributes/objectives which is done by the stakeholders. As said, the assignment of weights is beyond the scope of this research, but score of the PMs is within the scope. A suggested score can be obtained for each PM by calculating the percentage checks that are met out of the total number of checks. However, other performance scales can be used to obtain a score for a PM, preferably in cooperation with the relevant stakeholders.

Table 1. Performance Measure 6.2 for *Contractor Management*. There are three requirements for well performed contractor management

Are suppliers and contractors well chosen and monitored?
□ Do contractors/partners in the supply chain also need to have a BCM programme?
□ Is there somebody in the organization responsible for checking the current and near future circumstances of contractors and their performances?
□ Does the organization try to avoid the use of contract or outsourced employees for critical processes? If not: are measures taken to prevent outsourced employees from making failures / errors in the organization?

3 VALIDATION

3.1 Validation of Questions in the Checklist

As said, the development of the PM is based on various sources stemming from High Reliability Organizations, the British Standard 25999 (BSI, 2007) and the like. This ensures the completeness of the checklist. Though some were based on best practices, three companies (two IT departments, one parcel distributor) have been visited to test the applicability of the questions and refine them where needed. These companies have had experience with business continuity management so that they were able to provide feedback. The final checklist consists of 115 elements divided over 21 PMs or attributes. The authors realize that this is limited validation in terms of statistics. The overall impression is positive but more case studies are needed for further validation.

3.2 Validation of Performance Measures Completeness

Sixty-seven events and practices from case studies derived from 'The Resilient Enterprise' (Sheffi, 2005) have been used to test whether the cases were addressed by one or more PMs. 26 out of the 67 cases were not addressed by the PMs. The reason is that these cases refer to market risks, such as changing market conditions, demand fluctuations, forecasting problems, all outside the scope of this research. However, some strategies to deal with market risks are also used for coping with disruptions in the operational process. Examples are standardization of parts or facilities and redundant capacity. Future research may concentrate on integrating market (and other) risks in the value tree. The remaining 41 cases were all addressed by the PMs and validate the completeness of the lower structure of the value tree.

4 CONCLUSION

The intention of this research was to develop a method to assess operational resilience covering all relevant aspects rather than a fragmented approach. The methodology used is the multi-attribute utility theory and resulted in a value tree of operational resilience. The lowest-level attributes of this tree can be measured by checklists developed for this

research. This checklist was found significant in auditing resilience within three companies. In addition, the completeness of the value tree has been validated by 41 case studies from Sheffi (2005). The possibility to assign weights to attributes has not been presented in this research. The value tree given in this paper may be used as a steppingstone to include weighing of attributes and higher-level objectives. Additionally, other types of risks besides operational risks may be included in the value tree, such as the market risks.

REFERENCES

Apostolakis, G.E., Lemon, D.M. (2005). A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Analysis,* Vol. 25 (2), pp. 361-376.

British Standard Institute (BSI) (2007). British Standard 25999 – part 2.

Callagher, M. (2003). *Business Continuity Management – How to protect your company from danger*. Pearson Education Limited: London. ISBN 0-273-66351-8.

Chapman, R.J. (2006). *Simple Tools and Techniques for Enterprise Risk Management*. ISBN-10: 0-470-01466-0.John Wiley & Sons, Ltd.

Clemen, R.T. (1991). *Making Hard Decisions.* Belmont, CA: Duxbury Press.

Fiksel, J. (2006). Sustainability and Resilience: towards a systems approach. *Sustainability: Science, Practice, and Policy,* Vol. 2 (2), pp.14-21. http://ejournal.nbii.org, last visited March 11, 2008.

Flin, R. (2006). "Erosion of Managerial Resilience: From Vasa to NASA". In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds). *Resilience Engineering, concepts and precepts.* ISBN 0-7546-4641-6. Hampshire: Ashgate Publishing Limited, pp. 229-233.

Forman, E., Selly, M.A. (2001). Decision by Objectives. ISBN: 9810241437.

Klein, R.J.T., Nicholls, R.J., Thomalla, F. (2003). The Resilience of Coastal Megacities to weather-related hazards. In: Kreimer, A., Arnold, M., Carlin, A. (Eds). *Building safer cities: The future of disaster risk.* The World Bank Disaster Management Facility Washington D.C. www-wds.worldbank.org, last visited March 14, 2008.

McDonald, N. (2006). *Organizational Resilience and Industrial Risk.* In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds). *Resilience Engineering, concepts and precepts.* ISBN 0-7546-4641-6. Hampshire: Ashgate Publishing Limited, pp 155-180.

McManus, S., Seville, E., Brunsdon, D., Vargo, J. (2007). Resilience Management. Resilient Organizations Research Report 2007/01. www.resorgs.org.nz, last visited March 19, 2008.

Sheffi, Y. (2005). The Resilient Enterprise: overcoming vulnerability for competitive advantage. ISBN 0-262-19537-2. Cambridge: The MIT Press.