Calculation of Unpredictable Time Deviation from Defined Enterprise Information System Recovery Effort in Emergency Situations

Athanasios Podaras[1]

[1] **Department of Informatics, Technical University of Liberec**
Liberec, Czech Republic

Abstract

The present paper deals with creation of a model which estimates the negative impact of an unexpected factor on an enterprise information system recovery process, which is planned by the Business Continuity Management teams, towards a system outage caused by another foreseen crisis event. The core hypothesis of the contribution is the simultaneous occurrence of an unexpected factor during the information system restoration procedure, after a failover triggered by a crisis situation, for which the action steps are delineated in the Business Continuity Plan. In such case, the unexpected factor can negatively influence the estimated Recovery Time Effort (RTE) of the corresponding IT Business Process. Important part of the current work is the calculation of the approximate time deviation from the initially planned recovery time of the business function. The developed model is based on the Composite Risk Index theory of Risk Management.

Keywords: *Information System Recovery, IT Business Function, Business Continuity Plan, Crisis Situations, Unexpected Factor (UF), Composite Risk Index (CRI), Unexpected Factor Index (UFI).*

1. Introduction

The modern enterprise environment is fully characterized by the presence of multiple and complex information systems and software applications, as well as the indispensable dependence of the majority of critical business functions on such technological tools. However, multiple authors underline and strongly support not only the dependence of modern business functions on technology, but also, the parallel emergence of new enterprise operational threats due to computer based everyday core business tasks.

“Information Age” has not only brought international terrorism, but also an increased awareness of new types of contingencies - breakdown of information and communication systems, energy black-outs, emergence of natural threats, bio-nuclear terrorism, etc.[1]. Additionally, Mitroff and Anagnos [2], among 10 different major types of crisis, highlight the importance and the presence of the informational types (loss of proprietary information). Furthermore, Castillo [3] states that as businesses increasingly rely on data, information and technology, new threats are constantly emerging that affect all corporations. At the same time other experts and practitioners highlight the advantages provided by technology against such threats. Today’s information and communication technologies provide the means for improving prevention and recovery in many different ways [4].

According to the above scientific aspects stated by modern experts on the Crisis Management field, it can be concluded that one of the most important, and nowadays obligatory, tasks of the modern enterprises and organizations is the development and the establishment of an efficient and effective Business Continuity Management [5].

Key issue of a successful and effective business continuity plan, is the periodic execution of recovery exercises [6]. However, efficiently planned business continuity tests with regard to immediate IT System Recovery, should always include hard scenarios, according to which the corresponding business functions might not be easily recovered due to the emergence of several unexpected factors apart from the initial emergency situation scenario. In other words, exercise simulation to real crisis should involve scenarios according to which, an additional to the emergency case unexpected factor causes significant or unimportant, depending on the type of the factor, time deviation from the defined by the Business Plan the Rational Time Objective (RTO) [7], or, in the worst case, the Maximum Acceptable Outage (MAO) [7].

The present article deals with the development of a model which will be utilized towards the approximate calculation of the additional time required to restore an enterprise business function and its connected software applications during a crisis situation. The model includes RTO and MAO values defined by the enterprise business continuity strategy, the simultaneous emergence of an additional

Unexpected Factor apart from the emergency situation included in the business continuity testing scenario, and also, the calculation of the additional time required to recover the information system, the involved applications and the entire business function according to the unplanned and possibly extreme circumstance. The calculation of the aforementioned time deviation as well as the total time of the Recovery Time Effort (RTE) required is based on the Composite Risk Index Theory of Risk Management.

2. Model Description

As it was above stated, the core concept of the proposed contribution, is based on the hypothesis that an *Unexpected Factor (UF)* occurs during the information system recovery procedure, which was caused by a *Defined Factor (DF)*. For instance, it can be assumed that an electricity or network outage (Defined Factor DF) triggers an information system failover which may not be easily restored if, in a real similar event, there is lack of experienced and trained personnel (Unexpected Factor UF). The UF will significantly influence the demanded Recovery Time Effort (RTE) to recover the system the corresponding business functions. The expected Recovery Time is based on the Rational Time Objective (RTO) and the Maximum Acceptable Outage (MAO) values of the Business Continuity Plan. The model includes Unexpected Factor Impact Levels and Assessment Values, which are mapped to the Type of the UF. Moreover, the Time Deviation (TD) caused by the additional UF, IS calculated to the assessment value and the possibility of occurrence of the UF.

2.1 The Unexpected Factor (UF) Impact Level and Assessment Values

According to the proposed model, the *Unexpected Factor* is categorized in 4 different *Types.* The *Impact* or *Severity Level* of the Factor is mapped to the corresponding *Category Type* and *Assessment Value* (Tab. 1)

Table 1: List of UF Types

Impact/Severity Level	***Unexpected Factor Category Type***	***Assessment Value***
Very High	Extreme Type	4
High	Serious Type	3
Middle	Unusual Type	2
Low	Normal Type	1

An example of Extreme Factor scenario can be a Hurricane, if we refer to *weather conditions*, or long lasting extreme snowfall, which hardens the system recovery process if the initial emergency event that caused the information system outage is i.e. electricity outage, or network unavailability. Another example of Extreme Unexpected Factor, is the lack of personnel. An information system failure could may occur when all specialized and trained staff unexpectedly suffers from illness.

The detailed documentation of all possible UF's is a subject of another study. The present study focuses only on the creation of the model that calculates time deviation from the initially planned Recovery Time Effort (RTE). Thus, in the current paper, only the Category Types and the corresponding Impact Levels and Assessment Values are listed.

3. Derivation of the Unexpected Factor Index (UFI) from the Composite Risk Index CRI)

The current model includes the introduction and presentation of a new contribution to the IT Business Continuity Management research area, entitled as *Unexpected Factor Index (UFI).* The estimation of the specific index is based on the *Composite Risk Index (CRI)* notation, which stems from the most widely accepted formula for risk quantification [8], which is the following (Eq.1):

$$\mathit{RISK\ MAGNITUDE} = \mathit{RATE}\ (\mathit{or\ PROBABILITY})\ \mathit{OF\ OCCURENCE} \times \mathit{IMPACT\ OF\ EVENT} \tag{1}$$

Similarly, the *Composite Risk Index (CRI)* is calculated according to the following formula (Eq. 2):

$$\mathit{COMPOSITE\ RISK\ INDEX} = \mathit{IMPACT\ OF\ RISK\ EVENT} \times \mathit{PROBABILITY\ OF\ OCCURENCE} \tag{2}$$

According to the Composite Risk Index theory, the Impact is marked with a scale from 1 to 5, where 1 is the minimum impact value and 5 is the maximum impact value. Moreover, the probability of occurrence is also marked with a 5-level scale, and value 1 refers to the minimum probability, while 5 refers to the maximum probability of occurrence. As a result, it can be easily realized that the minimum value for CRI is 1 and the maximum value of CRI is 25.

For the estimation of the Unexpected Recovery Index (URI), a modification of the CRI model was implemented by the author. Since each UF is marked according to a 4-level scale (Tab. 1) of assessment values, the calculation of the UFI value shall be oriented to the specific scale. Thus, according to the delineated model, minimum impact value is 1 while maximum impact value is 4. For Possibility of Occurrence of each UF, a similar 4-level scale is determined.

As a result, the formula according to which the UFI is calculated will be the following (Eq. 3):

$$UFI = AV \times P \qquad (3)$$

where, AV = Assessment Value and P = Probability of Occurrence

According to Equation (3) and data obtained by Fig.1, the minimum and the maximum URI values regarding each factor are: $UFI_{MIN} = 1$ and $UFI_{MAX} = 16$.

Probability of Occurrence of UF	1	2	3	4
Assessment Value of UF	**Unexpected Factor Index (UFI) Of Each UF Modifier**			
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Fig. 1: Calculation of UF Index according to Assessment Value and Probability of Occurrence of a Factor

4. Calculation of Recovery Time Deviation (RTD) from Initially Defined Recovery Time Effort (RTE)

The final Part of the Model includes the Calculation of the approximate *Recovery Time Deviation (RTD)*. Under the assumption that the demanded Recovery Time Effort (RTE) in order to restore an information system, the involved applications and the corresponding business function is *X* hours (RTE = X), the same recovery procedure, in case of the occurrence of an Unexpected Factor (UF) will be undoubtedly prolonged. In this occasion, the RTD value will be calculated according to Eq. 4:

$$RTD = RTE \times \frac{UFI}{100} \qquad (4)$$

Consequently, the Total Recovery Time Effort will be estimated with the derived Eq. 5:

$$TRTE = RTE + RTD = RTE + RTE \times \frac{UFI}{100} = RTE\ (1 + \frac{UFI}{100}) \qquad (5)$$

An obvious conclusion which can be derived from the above Eq. (5) and from the fact that the Maximum Value of the UF is equal to 16, it can be assumed that the maximum value of the TRTE is calculated by the following formula (Eq. 6):

$$TRTE_{MAX} = 1.16 \times RTE \qquad (6)$$

A simple example of the proposed model can be the following:

Crisis Scenario 1 (Only Defined Factor DF considered):
An electricity failure triggers an information system which supports online transactions with suppliers.
The system performs critical transactions, and the determined by the Business Continuity Team Rational Time Objective (RTO) and Maximum Acceptable Outage (MAO) values are the following:
RTO = 2 Hours
MAO= 10 Hours
According to the executed recovery exercise, the result was that Recovery Time Effort (RTE) was,
RTE = 7 Hours.
Crisis Scenario 2 (Unexpected Factor Included):
In this case the RTO and MAO values should include the *worst case scenario*, according to which an Unexpected Factor occurs with UFI = 16. This means that for instance, an electricity outage occurs during a simultaneous extreme hurricane takes place, and the disaster recovery trained team cannot easily reach the backup recovery site due to the specific weather conditions.
In this case, the following results will be obtained:
RTO = 2 × 1.16 = 2.32 Hours
MAO = 10 × 1.16 = 11.6 Hours

If the Business Continuity Exercise will show that $TRTE_{MAX} >$ 11.6 Hours then the BC Strategic Plan should be modified.
If $TRTE_{MAX} <=$ 11.6 Hours then the BC Strategic Plan should be retained as is.

The above calculation methodology, is proposed by the author as a comparative value with the Maximum Acceptable Outage of a business function, which is determined by the Business Continuity Team of the enterprise or the organization.

4. Conclusions

The study analyzed in the present paper includes the development of a model which estimates the Time Deviation from the initially planned effort, required to recover an enterprise information system and its involved business functions during a crisis situation. The model includes the estimation of an additional Unexpected Factor which may occur during a real emergency event. Scenarios which are considered in terms of a Business Continuity Plan should always include the implementation of such cases. The present work included part of the entire model which is the list of Unexpected Factor (UF) categories, according to the impact level and corresponding assessment value of the factor, and also the calculation of the Recovery Time Deviation from the initially planned Recovery Time Effort (RTE), based on the RTO and MAO values of the Business Continuity Management. Future work will include the detailed definition of specific Unexpected Factors, which will be documented in a developed Software Application. The specific Software will automatically calculate the Recovery Time Deviation and Total Recovery Time Effort of the information system recovery during a crisis situation.

Acknowledgments

The present work is supported by ESF operational program "Education for Competitiveness" in the Czech Republic in the framework of project „Support of engineering of excellent research and development teams at the Technical University of Liberec“ No. CZ.1.07/2.3.00/30.0065.

References

[1] A. Boin, P. Hart, E. Stern and B. Sundelius, The Politics of Crisis Management: Public Leadership Under Pressure, Cambridge University Press, ISBN 0-521-84537-8, 2005

[2] I. Mitroff and G. Anagnos, "Managing Crisis before They Happen: What Every Executive Manager Needs to Know about Crisis Management", in AMACOM, 2001

[3] C. Castillo, " Disaster Preparedness and Business Continuity Planning at Boeing: An Integrated Model", Journal of Facilities Management, Vol. 3, No. 1, 2004, pp. 8-26.

[4] G. Chroust and D. Finlayson, "Reacting Systematically to Regional Disasters", in Invitation for Workshop at the ISSS Congress in Hull, UK, 2011

[5] Y. Asnar and P. Giorgini, "Analyzing Business Continuity through a Multi-Layer Model", in BPM ’08: Proc. Of the Int. Conf. on Business Process Management, pp. 212-227, Springer, 2008.

[6] Business Standard Institute, Exercises for Excellence, 2008

[7] Business Standard Institute, BS ISO 22301: 2012, 2012

[8] M. Ciobanu and M. Mazilu, "Environmental Crisis Management through Risk Management, Recent Researches in Tourism and Economic Development," in WSEAS 1st International Conference on Tourism and Economic Development (TED '11), Romania, 2011.

Athanasios Podaras is currently a Postdoctoral Researcher at the Department of Informatics, Faculty of Economics, Technical University of Liberec, Czech Republic. He received a Ph.D diploma in Information Management (2010) and an MSc Degree in System Engineering and Informatics (2005) from the Economic Faculty, Department of Information Engineering at the Czech University of Life Sciences in Prague, Czech Republic.